BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, D.C. 20554

In the Matter of: Petition of Telcordia Technologies, Inc. To Reform Amendment 57 and To Order a Competitive Bidding Process for Number Portability Administration	WC Docket No. 07-149
Petition of Telcordia Technologies, Inc. To Reform or Strike Amendment 70, To Institute a Competitive Bidding for Number Portability Administration, and To End the LLC's Interim Role in Number Portability Administration Contract Management	WC Docket No. 09-109

EX PARTE REPLY OF TELCORDIA TECHNOLOGIES, INC. TO THE EX PARTE RESPONSE OF NEUSTAR, INC.

John T. Nakahata
Linda McReynolds
Madeleine V. Findley
WILTSHIRE & GRANNIS LLP
1200 18th Street NW
Washington, DC 20036
(202) 730-1320

Counsel for Telcordia Technologies, Inc.

February 16, 2010

BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, D.C. 20554

In the Matter of: Petition of Telcordia Technologies, Inc. To Reform Amendment 57 and To Order a Competitive Bidding Process for Number Portability Administration	WC Docket No. 07-149
Petition of Telcordia Technologies, Inc. To Reform or Strike Amendment 70, To Institute a Competitive Bidding for Number Portability Administration, and To End the LLC's Interim Role in Number Portability Administration Contract Management	WC Docket No. 09-109

EX PARTE REPLY OF TELCORDIA TECHNOLOGIES, INC.
TO THE EX PARTE RESPONSE OF NEUSTAR, INC.

SUMMARY

NeuStar's ex parte response of December 8, 2009 ("NeuStar ex parte response")[1] asks this Commission to set aside the longstanding preference of the Congress, the President and the Federal Communications Commission ("Commission" or "FCC") for competitive bidding. Instead, NeuStar asks this Commission to believe that extending what was originally bid as a five-year contract for an additional thirteen years through non-competitive, non-transparent sole-source procurements conducted entirely behind closed doors has resulted in the best deal possible for consumers. NeuStar asks too much. Competition ensures that costs to taxpayers

[1] *See* Ex Parte Response to the Reply Comments of Telcordia Technologies, Inc., WC Docket No. 09-109, at iii (filed December 9, 2009) ("*NeuStar Ex Parte Response*"). Telcordia notes that this ex parte response was not contemplated in the Commission's comment schedule as issued in the Public Notice.

will be minimized. And "the public interest is clearly served when suppliers engage in fair and robust competition for government contracts."[2] Nothing about number portability database administration provides any basis for concluding that the public's interest is not best served by the vigorous and open competition that competitive bidding provides. Indeed, the most recent closed-door deals struck between NeuStar and the North American Portability Management, LLC ("NAPM"), Amendment 70, confirmed that their previous closed-door deal – Amendment 57 – was overpriced by at least 20% – just as Telcordia alleged in 2006.

NeuStar argues that the Commission should not order this contract to be put out for competitive bid for the first time since 1996 because NeuStar has lowered its per-transaction rate over the years. But unit prices *should* have come down: Number portability database administration is largely a fixed-price, fixed-cost service that has seen transaction volumes explode. Tellingly, the total bill for number portability administration has continued to increase – and will be nearly $500 million by 2015. NeuStar has used these unit price reductions to extract *de facto* exclusivity through at least 2015. And no one – including NAPM – has committed not to engage in yet another sole-source, non-transparent, behind-closed-door contract extension with NeuStar before 2015.

This Commission has inherited NeuStar's overly-rich contract, and it has the full power to fix it. Under Section 251(e), the Commission has the authority to designate number portability administrators. That necessarily comes with the power to *undesignate* NeuStar, as the contract that NeuStar's predecessor entered into with NAPM expressly recognized.

This Commission's predecessors did not and could not delegate all policymaking aspects of overseeing the number portability administrator to the North American Portability

[2] *Global Computer Enters., Inc. v. United States*, 88 Fed. Cl. 350, 461 (2009) ("*GCE*").

Management LLC ("NAPM LLC") without any guidance whatsoever. Nor did the Commission give NAPM leave to extend, amend and alter NPAC administrator contracts for as long as and on whatever terms it sees fit without any competitive bidding or prior approval by the Commission. But NeuStar breathtakingly claims the Commission's decision to allow the NAPM LLC to "manage and oversee" the NPAC administrator contracts on an interim basis did just those things. Such an expansive delegation of power is not supported by statute, the Commission's decisions or sound public policy. Moreover, the NeuStar number portability contract is not a private contract; it is funded through the Commission's exercise of the police power –requiring carrier payments by Commission rule, subject to Commission forfeitures for non-payment.

NAPM and NeuStar also are attempting to evade Congress' requirement through the Competition in Contracting Act for full and open competition for government contracts. In particular, CICA prohibits making "cardinal changes" to a contract – including changes that extend the term of a contract, enlarge its scope or change its fundamental pricing structure – without going through a new bidding process. In entering contract modifications that made such cardinal changes, NAPM violated CICA's requirements.

The core of this dispute, however, is the basic question of what should be the process to make fundamental decisions about when to expand the scope of the number portability database provider contract either in duration or in the scope of permitted activities, and who – NAPM or the FCC – should decide when to conduct competitive bidding and whether to reintroduce competition into number portability administration. These are policy questions affecting not just NAPM's members, but millions of consumers that pay these fees through their service rates or bottom-of-the-bill surcharges. NeuStar's contract now has been extended without rebidding for a cumulative period that – if not changed – will extend for at least thirteen years beyond the

contracts' initial term. This cannot constitute sound administration – and cannot provide the assurance that the Commission should require that number portability administration is being provided at the highest quality and the lowest price.

In the end, it falls to this Commission to restore transparency and accountability to number portability administration – and to restore the use of competitive bidding to safeguard both providers and consumers. The President, in his first two months in office could not have been clearer: "Excessive reliance by executive agencies on sole-source contracts (or contracts with a limited number of sources) and cost-reimbursement contracts creates a risk that taxpayer funds will be spent on contracts that are wasteful, inefficient, subject to misuse, or otherwise not well designed to serve the needs of the Federal Government or the interests of the American taxpayer."[3] Government contracts cases make clear that the appropriate remedy for improperly awarding a contract through sole-source procurement is to terminate that contract and to conduct a new competitive bid. That is exactly what this Commission should do here, and it is the only way to restore credibility and accountability to number portability administration.

[3] Memorandum for the Heads of Executive Departments and Agencies, 74 Fed. Reg. 9755, 9755 (Mar. 4, 2009).

TABLE OF CONTENTS

INTRODUCTION 1

ARGUMENT 5

I. NEUSTAR'S PERFORMANCE HISTORY AND UNIT PRICE CUTS ARE NOT A REASON TO FOREGO THE BENEFITS OF OPEN, TRANSPARENT COMPETITIVE BIDDING IN FAVOR OF CLOSED-DOOR, NON-TRANSPARENT, SOLE-SOURCED PROCUREMENTS. 5

II. THE COMMISSION HAS THE AUTHORITY AND THE BASIS FOR SETTING ASIDE OR DIRECTING REVISIONS TO THE NPAC CONTRACT AS CONTRARY TO THE PUBLIC INTEREST. 6

III. THE COMMISSION *DID NOT*, AND *CANNOT*, DELEGATE POLICYMAKING AUTHORITY OVER THE NUMBER PORTABILITY CONTRACT TO NAPM OR THE NANC. 10

IV. NEUSTAR IS ATTEMPTING TO EVADE CICA'S REQUIREMENTS FOR FULL AND OPEN COMPETITION FOR GOVERNMENT PROCUREMENT CONTRACTS. 16

V. NAPM MUST COMPLY WITH CICA'S COMPETITIVE BIDDING REQUIREMENTS. 19

A. The NAPM LLC is a Public Instrumentality. 21

B. The NAPM LLC is Not a Prime Contractor. 24

C. The NPAC Contract Involves the Use of Public Funds. 25

D. The NPAC Contract is a Procurement for Government Services. 27

E. The Contract Modifications are Outside the Scope of the Original Procurement. 29

CONCLUSION 35

BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, D.C. 20554

In the Matter of: Petition of Telcordia Technologies, Inc. To Reform Amendment 57 and To Order a Competitive Bidding Process for Number Portability Administration	WC Docket No. 07-149
Petition of Telcordia Technologies, Inc. To Reform or Strike Amendment 70, To Institute a Competitive Bidding for Number Portability Administration, and To End the LLC's Interim Role in Number Portability Administration Contract Management	WC Docket No. 09-109

EX PARTE REPLY OF TELCORDIA TECHNOLOGIES, INC.
TO THE EX PARTE RESPONSE OF NEUSTAR, INC.

INTRODUCTION

NeuStar's ex parte response of December 8, 2009 ("NeuStar ex parte response")[4] asks this Commission to set aside the longstanding preference of the Congress, the President and the Federal Communications Commission ("Commission" or "FCC") itself for competitive bidding, and to believe that extending what was originally bid as a five-year contract for an additional thirteen years through non-competitive, non-transparent sole-source procurements conducted entirely behind closed doors has resulted in the best deal possible for consumers. NeuStar asks

[4] *See* Ex Parte Response to the Reply Comments of Telcordia Technologies, Inc., WC Docket No. 09-109, at iii (filed December 9, 2009) ("*NeuStar Ex Parte Response*"). Telcordia notes that this ex parte response was not contemplated in the Commission's comment schedule as issued in the Public Notice.

too much. As courts have recognized, "'healthy competition ensures that the costs to the taxpayer will be minimized'" and "the public interest is 'clearly served when suppliers engage in fair and robust competition for government contracts.'"[5] "The 'public has an interest in honest, open[,] and fair competition,'"[6] and"[w]henever a [potential bidder] is improperly excluded from that process, that interest is compromised."[7] There is nothing about number portability database administration that provides any basis for concluding that the public's interest is not best served by the vigorous and open competition that competitive bidding provides. Indeed, the most recent closed-door deals struck between NeuStar and the North American Portability Management, LLC ("NAPM"), Amendment 70, confirmed that their previous closed-door deal – Amendment 57 – was overpriced by at least 20% -- just as Telcordia alleged in 2006.

NeuStar argues that the Commission should not order this contract to be put out for competitive bid for the first time since 1996 because NeuStar has lowered its per transaction rate over the years. But the unit price reductions should come as no surprise: Number portability database administration is largely a fixed-price, fixed-cost service that has seen transaction volumes explode. Unit prices should have come down. Tellingly, what has continued to increase is the total bill for number portability administration – which will be nearly $500 million by 2015. And NeuStar has cleverly used these unit price reductions to extract *de facto* exclusivity through at least 2015 and to allow it to use the monopoly NPAC to enter other, competitive markets. No one – including NAPM – has made any commitment that NAPM will not engage in yet another sole-source, non-transparent, behind-closed-door contract extension

[5] *Global Computer Enters., Inc. v. United States*, 88 Fed. Cl. 350, 461 (2009) ("*GCE*").

[6] *Magellan Corp. v. United States*, 27 Fed. Cl. 446, 448 (1993).

[7] *GCE*, 88 Fed. Cl. at 461.

with NeuStar before 2015 that will further delay putting this contract to the market test of competitive bidding required by law, sound procurement policy and common sense.

NeuStar would have this Commission believe that it is powerless to put a stop to a problem it did not create. But that is not true. This Commission may have inherited NeuStar's overly-rich contract, but it has the full power to fix it. Under Section 251(e), the Commission has the authority to designate number portability administrators – a power it exercised when it designated NeuStar's predecessor as an Administrator. That necessarily comes with the power to *undesignate* NeuStar, or to designate other Administrators to compete with NeuStar. Indeed, the contract that NeuStar, through its predecessor, Lockheed Martin IMS, entered into with NAPM in 1997 expressly recognized that the FCC could at any time alter its structure for number portability administration – and the contract expressly contemplated that NPAM could terminate its contract with NeuStar if required by a regulatory change.

NeuStar would also have this Commission believe that its predecessors delegated all policymaking aspects of overseeing the number portability administrator to the North American Portability Management LLC ("NAPM LLC") – a private group of large carriers – without any guidance whatsoever. NeuStar's ex parte response further asks this Commission to believe that it thereby left the NAPM to extend, amend and alter NPAC administrator contracts for as long as and on whatever terms it sees fit without any competitive bidding or prior approval by the Commission. Again, NeuStar goes too far. NeuStar bases this breathtaking assertion solely on the Commission's decision to allow the NAPM LLC to "manage and oversee" the NPAC administrator contracts on an interim basis. But such an expansive delegation of power is not supported by statute, the Commission's decisions or sound public policy – and the Commission should not interpret its earlier orders as having done so. After all, the NeuStar number

portability contract is funded through the Commission's exercise of the police power – setting the formula for carrier contributions and requiring such payments as a matter of Commission rule, subject to Commission forfeitures for non-payment.

NAPM and NeuStar together are attempting to evade Congress' requirement through the Competition in Contracting Act for full and open competition for government contracts. In particular, CICA prohibits making "cardinal changes" to a contract – including changes that extend the term of a contract, enlarge its scope or change its fundamental pricing structure – without going through a new bidding process. In entering contract modifications that made such cardinal changes, NAPM violated CICA's requirements.

The core of this dispute, however, is not the technicalities of CICA. It is the basic question of what should be the process to make fundamental decisions about when to expand the scope of the number portability database provider contract either in duration or in the scope of permitted activities, and who – NAPM or the FCC – should decide when to conduct competitive bidding and whether to reintroduce competition into number portability administration. These are policy questions that affect not just NAPM's members – and not even just the thousands of carriers that are required by FCC rule to pay NeuStar – but millions of consumers that pay these fees through their service rates or bottom-of-the-bill surcharges. NeuStar's contract now has been extended without rebidding for a cumulative period that – if not changed – will extend for at least thirteen years beyond the contracts' initial term. This cannot constitute sound administration – and cannot provide the assurance that the Commission should require that number portability administration is being provided at the highest quality and the lowest price.

In the end, it falls to this Commission to restore transparency and accountability to number portability administration – and to restore the use of competitive bidding to safeguard

both providers and consumers. The President, in his first two months in office could not have been clearer: "Excessive reliance by executive agencies on sole-source contracts (or contracts with a limited number of sources) and cost-reimbursement contracts creates a risk that taxpayer funds will be spent on contracts that are wasteful, inefficient, subject to misuse, or otherwise not well designed to serve the needs of the Federal Government or the interests of the American taxpayer."[8] Government contracts cases make clear that the appropriate remedy for improperly awarding a contract through sole-source procurement is to terminate that contract and to conduct a new competitive bid. That is exactly what this Commission should do here, and it is the only way to restore credibility and accountability to number portability administration.

ARGUMENT

I. NEUSTAR'S PERFORMANCE HISTORY AND UNIT PRICE CUTS ARE NOT A REASON TO FOREGO THE BENEFITS OF OPEN, TRANSPARENT COMPETITIVE BIDDING IN FAVOR OF CLOSED-DOOR, NON-TRANSPARENT, SOLE-SOURCED PROCUREMENTS.

NeuStar contends that because it consistently has performed as agreed, the Commission need not exercise its authority over the contract to ensure that charges are as low as possible. Additionally, NeuStar emphasizes that the contract modifications have resulted in lower per transaction costs for carriers, highlighting NeuStar's apparent beneficence in an attempt to distract attention from its cozy, uncompetitive contracting arrangement. But good performance is not a reason to forego a competitive bid, as performance quality can be both an evaluation criteria and a contract condition through service level guarantees. And these unit price reductions come as no surprise. The NPAC database is, after all, largely a fixed-price, fixed-cost service that has seen dramatically escalating volumes. Of course NeuStar would be willing to

[8] Memorandum for the Heads of Executive Departments and Agencies, 74 Fed. Reg. 9755, 9755 (Mar. 4, 2009).

reduce the per transaction price by some amount, particularly when volumes (and thus total revenues) have been increasing and it has been able to secure *de facto* exclusivity through 2015. The bottom line is that the total bill for running this largely fixed-cost operation has continued to escalate – and will reach nearly a *half billion* dollars *per year* by 2015.

After thirteen years without competition (and more by the time any transitions could occur), NeuStar has recovered its costs several times over and enjoyed substantial profits. The question that has not been answered – because competitive bidding has not occurred and these deals have been forged on a non-transparent, sole-source basis – is whether these price reductions are as good a deal as can be gotten. Sound procurement policy, both the principles and mandates of the Competition in Contracting Act, and the Commission's experience in bidding other parts of numbering administration strongly suggest that competitive bidding can yield better results, while being more transparent and fair to all potential vendors. Moreover, Telcordia's willingness to offer lower rates even in the unsolicited bid process shows that competitive bidding likely will result in substantial overall savings.

II. THE COMMISSION HAS THE AUTHORITY AND THE BASIS FOR SETTING ASIDE OR DIRECTING REVISIONS TO THE NPAC CONTRACT AS CONTRARY TO THE PUBLIC INTEREST.

The Commission's authority to order changes in number portability administration – including the termination of the NAPM-NeuStar contract – is straightforward. Section 251(e) gives the Commission "exclusive jurisdiction" over the NPAC. Under Section 251(e), the Commission has plenary authority over numbering policy.[9] Everyone agrees that the Commission has the statutory authority to designate an Administrator for local number portability pursuant to 47 U.S.C. § 251(e)(1). Nothing in the statute suggests the Commission's

[9] 47 U.S.C. § 251(e); *see also* 47 C.F.R. §§ 52.3, 52.15 *et seq.*

ability to end an Administrator's designation as such is limited in any way. The Commission's power to designate "one or more impartial entities to administer telecommunications numbering"[10] *necessarily* includes the authority to *un*designate an Administrator, so that it can designate a different Administrator if it so chooses.

Indeed, the position of NPAC Administrator – the role NeuStar performs under its contract with NAPM –is entirely a creature of the Commission and its number portability rules.[11] After the NANC made its recommendations as to which entities should be designated as the Administrator, it was the Commission that adopted those recommendations and designated NeuStar (then Lockheed Martin IMS) and Perot Systems as the administrators.[12] When Perot Systems failed, it was again the FCC that designated NeuStar the administrator for the remaining regions.[13] Nowhere was it ever suggested that these designations were irrevocable. To the contrary, both the Commission and the NANC expressly contemplated that there would be later competitive bidding for continuation in the role as administrator – which has not to date occurred, even though over thirteen years have elapsed since the initial bids.[14]

The Commission, in the exercise of its authority under Section 251(e), can issue an order advising NeuStar and participating carriers that the Commission intends to reevaluate its

---

[10] 47 U.S.C. § 251(e)(1).

[11] *In re Telephone Number Portability*, First Report and Order, 11 FCC Rcd. 8352,8400-8401, ¶¶ 92-93 (1996) ("*First LNP Order*").

[12] *In re Telephone Number Portability*, Second Report and Order, 12 FCC Rcd. 12281, 12303, ¶ 33 (1997) ("*Second LNP Order*").

[13] *In re Telephone Number Portability*, Second Report and Order on Reconsideration, 13 FCC Rcd. 21204, 21209 ¶ 9 (1998).

[14] *See, e.g.*, Second LNP Order, 12 FCC Rcd. at 12305 ¶ 36 ("Second, the NANC observes that having multiple database administrators permits competition in both the initial and future competitive bidding and selection processes, which should enable carriers to obtain more favorable terms and conditions than if only one database administrator had been selected.")

Administrator designation pursuant to an open and competitive bidding process, and that it intends to do so immediately. The Commission need not conduct a rulemaking to do so, because no changes to its rules are necessary to undertake such an action. The Commission need only have a rational basis for its action, which the record in this docket more than supplies.[15]

Furthermore, the NAPM/NeuStar Master Agreement makes clear that NeuStar never had any reasonable expectation that it could not be subject to termination of its agreements by FCC action. To the contrary, in the Master Agreement, NAPM and NeuStar both have recognized the Commission's authority. Article 25 of the Master Agreement provides, "Contractor [NeuStar] expressly recognizes that (i) Customer [NAPM], Members and the Users and the NPAC/SMS are or may be subject to certain federal and state statutes and rules and regulations promulgated thereunder, as well as rules, regulations, orders, opinions, decisions and possible approval of the FCC, NANC and other regulatory bodies having jurisdiction or delegated authority over Customer, Member and the Users and the NPAC/SMS and (ii) this Agreement is subject to changes and modifications required as a result of any of the foregoing."[16] Article 25 additionally provides that NAPM "may terminate this Agreement if the required amendment or Statement of Work is technically or economically unfeasible or if the regulatory change requires Customer to terminate this Agreement."[17] Further, Article 23 gives NAPM the right to "terminate this Agreement or any applicable Statements of Work . . . under the circumstances related to a

[15] *See Nat'l Cable & Telecommc'ns Ass'n v. Fed. Commc'ns Comm'n*, 567 F.3d 659, 671 (D.C. Cir. 2009); Second LNP Order, 12 FCC Rcd. 12303 ¶ 33; Agreement for NPAC/SMS between Lockheed Martin IMS and Northeast Carrier Acquisition Company Arts.23-25 ("*Master Agreement*").

[16] Master Agreement, Art. 25.1

[17] *Id*.

regulatory event as set forth in Article 25."[18] Article 24 then sets forth the process to be followed by NeuStar and NAPM in the event of termination, including obligating NeuStar to assist with a transition and terms to govern during a transition as a result of regulatory action.[19]

Accordingly, Section 251(e) provides the Commission with complete authority to terminate the NeuStar/NAPM agreements and initiate new competitive bids. The NeuStar/NAPM contract fully acknowledges the Commission's authority in this regard, and NeuStar therefore had no reasonable contractual expectation that such a Commission-ordered termination would not occur.[20]

[18] *Id*. at Art. 23.1.

[19] *Id*. at Arts. 24.1, 24.3.

[20] The Commission thus need not reach the issues of whether number portability database administration services are common carrier services, and whether they can be terminated as unjust and unreasonable practices under Section 201. However, as set forth in Telcordia's Petition and Reply, the number portability administration database is a common carrier service under Section 201 of the Telecommunications Act and thus the contract can also be terminated and put out for immediate competitive bid under Section 201, because its *de facto* exclusivity and inseverability clauses are unjust and unreasonable, and the modifications to include ENUM functionalities are unlawful under 47 C.F.R. 52.25(f). Section 201 further gives the Commission authority to regulate common carrier services. 47 U.S.C. § 201(a); *see also In re Toll-Free Service Access Codes*, Third Report & Order, 12 FCC Rcd. 23040, 23076, ¶ 71 (Oct. 9, 1997) ("Common carrier services include services offered to other carriers, such as exchange access service, which is offered on a common carrier basis and provided primarily to other carriers."). NeuStar incorrectly claims that the *Second LNP Order* somehow "rejected" this rationale, rendering § 201 inapplicable. NeuStar Ex Parte Response at 52. This fundamentally misreads the *Second LNP Order*. In the *Second LNP Order*, the Commission rejected Bell Atlantic's request for tariffing because the statute expressly provided for the Commission to determine the method for calculating the amount any particular carrier would pay for number portability. Second LNP Order, 12 FCC Rcd. at 12349-50 ¶ 124. This has no bearing on whether number portability services are common carrier services, just as the toll-free database services are. Moreover, the *Sierra-Mobile* doctrine gives the Commission authority – though no additional authority is needed beyond the contract itself – to abrogate the contract *to prevent harm to the public interest*. *See United Gas Pipe Line Co. v. Mobile Gas Serv. Corp.*, 350 U.S. 332 (1956); *Federal Power Comm'n v. Sierra Pac. Power Co.*, 350 U.S. 348 (1956); *see also NRG Power Mktg., LLC v. Maine Pub. Utils. Comm'n*, No. 08-674, __ U.S. __ (Jan. 13, 2010).

III. THE COMMISSION *DID NOT,* AND *CANNOT,* DELEGATE POLICYMAKING AUTHORITY OVER THE NUMBER PORTABILITY CONTRACT TO NAPM OR THE NANC.

The Commission *did not*, because it cannot, delegate its authority over policymaking for number portability administration to NAPM. Instead, the Commission merely designated NAPM's predecessors to "manage and oversee" the Number Portability Administrator (NeuStar) on an interim basis. The Commission additionally directed NANC to provide oversight to NAPM.[21] At all times, however, the Commission has retained plenary authority over both number portability and the entities overseeing and managing the NPAC database. Even NeuStar recognizes this, conceding that "[t]he Commission delegated to NANC the more limited role of reviewing and overseeing the LLCs' management of the LNPAs and reserved for itself review of NANC's oversight of the LLCs."[22] NeuStar relies on a distorted reading of the *Second LNP Order* to convert this into *carte blanche* license for NAPM to make any and all decisions with respect to the NPAC contracts.

The *Second LNP Order*, however, reiterates that the Commission retains plenary authority over number portability.[23] Indeed, the *Second LNP Order* states "the Commission retains ultimate authority over number portability matters."[24] Instead of delegating away its power, as NeuStar claims, the Commission in fact emphasized the limited time and scope of the management and oversight authority it had delegated to NANC and to NAPM.[25]

---

[21] "In addition, we adopt the NANC's recommendation that it provide ongoing general oversight of number portability administration, including oversight of the individual LLCs, subject to Commission review." Second LNP Order, 12 FCC Rcd. at 12345 ¶ 114.

[22] NeuStar Ex Parte Response at 9 (emphasis added); *see also id.* at 5-6 & n.16.

[23] Second LNP Order, 12 FCC Rcd. at 12351-52 ¶ 129.

[24] *Id*.

[25] *Id*. at 12345-46 ¶¶ 114-115.

> Specifically, we adopt, on an *interim* basis, the NANC's recommendation that the LLCs provide immediate oversight and management of the local number portability administrators. The LLCs should serve in this role until the Commission concludes a rulemaking to examine the issue of local number portability administrator oversight and management including, but not limited to, the question of whether the LLCs should continue to act in this capacity.[26]

Additionally, "we adopt the NANC's recommendation that it provide ongoing general oversight of number portability administration, including oversight of the individual LLCs, *subject to Commission review*."[27] Regarding the LLCs' oversight responsibilities, the Commission equally underscored the temporary nature of their roles. "We conclude that, at least in the *short term*, the LLCs should provide *immediate* oversight for the regional local number portability administrators."[28] This was because "the LLCs were responsible for negotiating the master contracts with their respective local number portability administrators," and thus were "the entity with the greatest expertise regarding the structure and operation of the database for its region."[29]

Accordingly, as NeuStar acknowledges,[30] the Commission concluded that as local number portability went into effect, "using an entity other than the LLC to provide immediate oversight of the local number portability administrator would waste the LLC's valuable expertise and run the risk that necessary modifications to the database system may be delayed."[31] Yet again, however, the Commission emphasized that "such oversight shall be on an interim basis."[32] And, always, "the Commission retains ultimate authority over number portability matters."[33]

---

[26] *Id*. at 12345 ¶ 114 (emphasis added).

[27] *Id*. (emphasis added).

[28] *Id*. at 12345-46 ¶ 115 (emphasis added).

[29] *Id.* at 12346 ¶ 117.

[30] NeuStar Ex Parte Response at 9-10.

[31] Second LNP Order, 12 FCC Rcd. at 12346 ¶ 117.

[32] *Id*. at 12346-47 ¶ 119.

[33] *Id*. at 12351-52 ¶ 129.

Nothing in the *Second LNP Order* suggests that the Commission was granting NAPM broad policymaking authority. Indeed, a broad delegation would be contrary to the Commission's power to appoint the Administrator. When delegating authority, the Commission normally states its intentions expressly and sets parameters on the delegated authority – as it has done when delegating number conservation authority to state public utility commissions.[34] In those instances, the Commission details the scope of the delegated authority, including any conditions or limitations thereon, and "requir[ing state commissions] to abide by the same general requirements that the Commission has imposed on the numbering administrator."[35] NeuStar contends that the existence of its change order process suggests that the Commission authorized NAPM to make fundamental policy changes. A change order process simply permits the parties to revise the way they accomplish the work within the scope of the original contract.[36] The existence of a change order process cannot and does not authorize NAPM to make fundamental policy changes.

---

[34] *See, e.g., In re New York State Department of Public Service Petition for Additional Delegated Authority to Implement Number Conservation Measures*, Order, CC Docket No. 96-98, FCC 99-247 (rel. Sept. 15, 1999) (setting forth specific delegations of authority to New State PSC to implement thousands-block number pooling); *In re New Hampshire Public Utilities Commission's Petition for Additional Delegated Authority to Implement Number Optimization Measures in the 603 Area Code*, Order, 15 FCC Rcd. 1252, 1255 ¶¶ 8-9 (1999) ("*New Hampshire Delegation Order*") (providing specific duties while also noting limitations on delegated authority); *Maine Public Utilities Commission Petition for Additional Delegated Authority to Implement Number Conservation Measures*, Order, CC Docket No. 96-98, FCC 99-260 (rel. Sept. 28, 1999) (same); *Massachusetts Department of Telecommunications and Energy's Petition for Waiver of Section 52.19 to Implement Various Area Code Conservation Methods in the 508, 617, 781, and 978 Area Codes*, Order, CC Docket No. 96-98, FCC 99-246, NSD File No. L-99-19 (rel. Sept. 15, 1999) (same); *see also In re Improving the Public Safety Communications in the 800 MHz Band et al.*, 19 FCC Rcd. 14,969 (Aug. 6, 2004) ("*800 MHz Order*");

[35] New Hampshire Delegation Order, 15 FCC Rcd. at 1255 at ¶8.

[36] *GCE*, 88 Fed. Cl. at 437-41.

NeuStar asserts that the Commission's delegation of a Transition Administrator (TA) in the 800 MHz transition parallels the number portability process. This mischaracterizes the TA's role and authority in multiple ways. First, the Commission gave specific, express guidance about the TA's duties and authority.[37] Second, the Commission directed the TA to enter a contract containing specific Commission-articulated provisions, and to submit that contract to the Commission "for review and approval prior to execution."[38] "[G]iven the *detailed guidelines* under which the coordinators and Transition Administrator will operate, coupled with the *procedures for ongoing Commission review*," the Commission "conclude[d] that Commission use of such expertise and services is well within [its] authority."[39] In contrast, no such detailed descriptions of NAPM's duties and authority exist, nor did the Commission require specific clauses in NAPM's contract with the NPAC database administrator or require Commission review and approval prior to execution. In fact, none of those factors is present here. Far from supporting NeuStar's position, the 800 MHz transition stands in stark opposition to local number portability. In the 800 MHz transition, unlike local number portability, the TA had specific, defined duties, was directed to contract for certain articulated responsibilities, and was closely overseen by the Commission. The open-ended language NeuStar relies on as authorization for its conduct is in no way analogous to the TA in the 800 MHz transition.

NeuStar's reliance on the possibility of Commission oversight to cure the delegation problems described above is highly ironic. Through clauses inserted in each contract modification, NeuStar consistently has sought to thwart such oversight. As discussed in Telcordia's Petition and Reply, NeuStar deliberately structured their contracts with inseverability

[37] 800 MHz Order, 19 FCC Rcd. at 303-04 ¶¶199-200.

[38] *Id*.

[39] *Id*., 19 FCC Rcd. at 304 ¶ 200 (emphasis added).

clauses that effectively hold captive the industry and insulate NAPM and NeuStar's overreaching from NANC or Commission review.[40]

Nonetheless, NeuStar suggests that 47 U.S.C. § 251(e)(1) permits the Commission to delegate all of its authority over LNP to NAPM or NeuStar. The statute, however, does not support this claim. Indeed, "[w]hat constitutes 'numbering administration' or is encompassed by the NANP under § 251(e), given the FCC's 'exclusive jurisdiction' and its authority to 'delegate to State commissions . . . all or any portion of such jurisdiction' is far from clear."[41] But in any event, § 251(e)(1) is not the expansive, unlimited grant of power that NeuStar suggests, but rather a limited grant of authority to the Commission to appoint NAPM to manage and oversee numbering portability. Had Congress intended to permit the Commission to delegate authority to private organizations, such as NAPM or NeuStar, it could have said so. NeuStar identifies just such an instance, where Congress explicitly permitted the Commission to "authorize the use of private organizations for testing and certifying" device compliance.[42]

In § 251(e)(1), Congress instead authorized delegation to "State commissions or other entities." Understood in the context of the statute, this delegation extended to governmental entities and their subordinates. Thus, the Commission may delegate authority to NANC, but not to the NAPM LLC. The *USTA* decision explains why this is true: "the case law strongly suggests that subdelegations to outside parties are assumed to be improper absent an affirmative

---

[40] Petition of Telcordia Technologies, Inc. To Reform or Strike Amendment 70, To Institute Competitive Bidding for Number Portability Administration, and To End the NAPM LLC's Interim Role in Number Portability Administration Contract Management, WC Docket Nos. 07-149, 09-109, 43-45 (filed May 20, 2009); Reply Comments of Telcordia Technologies, Inc., Docket No. 09-109, at 55-57 (filed Sept. 29, 2009).

[41] *New York v. Fed. Commc'ns Comm'n*, 267 F.3d 91, 103 (2d Cir. 2001).

[42] 47 U.S.C. § 302a(e)(1); *see also* NeuStar Ex Parte Response at 42.

showing of congressional authorization."[43] Noting that "[t]his distinction is entirely sensible," the *USTA* court further stated, "When an agency delegates authority to its subordinate, responsibility--and thus accountability--clearly remain with the federal agency. But when an agency delegates power to outside parties, lines of accountability may blur, undermining an important democratic check on government decision-making."[44] This is precisely what has occurred here.

Moreover, *USTA* accords with OMB Circular A-76: The Commission *cannot* delegate its fundamental policymaking authority to non-federal entities without expressly approving, and making the final judgment respecting, these decisions. At the core of governmental accountability is the fundamental principle that the federal government must make *inherently governmental* decisions.

Finally, NeuStar is correct that the Commission did not delegate to NAPM these inherently governmental decisions.[45] But NeuStar fails to explain or to justify NAPM's actions in negotiating twelve years of noncompetitive, no-bid contract extensions whose terms manifestly represent inherently governmental decisions. NAPM personnel are not governmental personnel, and NeuStar does not argue otherwise. Accordingly, the contract modifications

---

[43] *United States Telecom Ass'n v. Fed. Commc'ns Comm'n*, 359 F.3d 554, 565 (D.C. Cir. 2004) ("*USTA*").

[44] *Id*. *USTA* dealt with a challenge to the Commission's purported delegation of authority to state commissions. The *USTA* court distinguished between *Congressional* delegations to outside entities and *administrative* delegations to outside entities. The former might be permissible in certain circumstances, whereas the latter was not. "We therefore hold that, while federal agency officials may subdelegate their decision-making authority to subordinates absent evidence of contrary congressional intent, they may not subdelegate to outside entities--private or sovereign--absent affirmative evidence of authority to do so." *Id*. at 566.

[45] NeuStar Ex Parte Response at 46.

making cardinal changes to the Master Agreement violate settled case law and federal agency policy and should be rescinded and rebid.

IV. NEUSTAR IS ATTEMPTING TO EVADE CICA'S REQUIREMENTS FOR FULL AND OPEN COMPETITION FOR GOVERNMENT PROCUREMENT CONTRACTS.

NeuStar seeks to protect (and expand) its monopoly position as the sole NPAC database administrator. To that end, it has negotiated repeated amendments to the NPAC contract that in effect further expand that monopoly both in time (decades) and scope (moving into the IP space), and that entrench it by moving to a quasi-fixed price structure without new competitive bids. NeuStar insists that the subsequent substantial modifications and extensions of the contract are in some sense included in the competitive bidding process that took place fourteen years and many amendments ago. But these subsequent modifications to the contract have been so substantial in scope and scale as to be tantamount to a new contract. They must be subject to competitive bidding under the Competition in Contracting Act (CICA), as well as sound and well recognized contract management principles.[46]

In an effort to make this proceeding appear more complicated than it is, NeuStar complains that Telcordia has throughout this proceeding challenged various amendments to the Master Agreement.[47] But what Telcordia has been seeking is the opportunity actually to compete competitively to be a NPAC Administrator through an open and transparent, competitive bidding process. Telcordia has challenged each of the recent amendments – including Amendments 57, 70 and 72 – that have extended, expanded and transformed the NPAC contract into a *de facto* exclusive contract that runs through 2015. As courts have

[46] The Competition in Contracting Act of 1984, Pub. L. No. 98-369, 98 Stat. 1175 (codified at 10 U.S.C. § 2304 and 41 U.S.C. § 253).

[47] NeuStar Ex Parte Response at 11 n.46.

recognized, "The 'public has an interest in honest, open[,] and fair competition,"[48] and "[w]henever a plaintiff is improperly excluded from that process, that interest is compromised."[49] Moreover, "[h]ealthy competition ensures that the costs to the taxpayer will be minimized" and "the public interest is 'clearly served when suppliers engage in fair and robust competition for government contracts.'"[50] A look at the purpose and scope of the contract will suffice for the Commission to determine that this contract should be let out for bid subject to CICA's open and competitive bidding requirements and sound contracting principles.

CICA was enacted to protect against precisely the situation that led to this dispute. Congress "had grown concerned that federal agencies were overspending on goods and services by making noncompetitive procurements from a single vendor instead of reaping the natural cost benefits of a full and open competition among several vendors."[51] CICA therefore embodies the federal government's strong preference for full and open competition. It applies to the procurement of goods and services by the federal government and mandates that modifications beyond the scope of an initial contract must be openly and competitively bid.

Generally, open and competitive bidding involves publication of a notice specifying an agency's needs and the factors the agency will consider in assessing bids. NeuStar pleads with the Commission not to upset its sweetheart monopoly deal. It suggests that giving its competitors in the industry a chance to make competitively-bid, head-to-head proposals for NPAC database administration will send the Commission down a slippery slope of following procurement laws each and every time it confers a status or designation on any private entity,

---

[48] *Magellan Corp.*, 27 Fed. Cl. at 448.

[49] *GCE*, 88 Fed. Cl. at 461 (internal quotation marks and citation omitted).

[50] *Id*. (citation omitted).

[51] *Corel Corp. v. United States*, 165 F. Supp. 2d 12, 19 (D.D.C. 2001) (citing H.R. Conf. Rep. No. 861, at 1421 (1984), reprinted in U.S.C.C.A.N. 1445, 2109).

even for ministerial duties such as frequency coordination. Not so. The Commission's designation of administrators and coordinators in other instances has not violated CICA's requirements.[52] Furthermore, even if the Commission were to determine that additional services

[52] Applying CICA to the NPAC contract procurement does not require reevaluation of other FCC-delegated functions that NeuStar enumerates in its Ex Parte submission at pages 22-28.

First, the Toll Free database service was created and overseen by the LECs, who provided access to the database through federally filed tariffs, with Section 203 and other Title II protections. DSMI, a subsidiary of Telcordia, as the Toll Free Administrator and business manager for the LECS, manages the help desk, hardware, and software contracts, each of which is competitively bid. Telcordia has no objection to a competitive procurement for the Business Management contract, a contract that is valued at about $1.3 million per year, far less than the estimated value of $300-500 million per year for NeuStar's NPAC contract. ATIS's SNAC, not DSMI, recommends the rollout of additional toll free codes and the Commission approves any such rollout. *See Toll Free Service Access Codes*, 15 FCC Rcd. 11939, 11946 (2000).

Second, the LERG™ Routing Guide, unlike the NPAC database, is a private and proprietary Telcordia product. Competitive alternatives exist in the marketplace for this product. In addition, the LERG is a "routing administration" tool, not covered by the Communications Act as is number portability. There is no regulatory requirement for service providers to use the LERG Routing Guide and Telcordia cannot rely on FCC enforcement for collection of fee related to its routing administration services.

Third, the FCC's designation of a wireless medical telemetry service (WTMS) frequency coordination administrator followed a public notice seeking requests from parties interested in serving in that role. The frequency coordinator would only notify parties of potential conflicts. *See Wireless Telecommunications Bureau Opens Filing Window for Requests To Be a Frequency Coordinator in the Wireless Medical Telemetry Service*, Public Notice, 15 FCC Rcd. 19038 (2000). Thus the frequency coordinator had only constrained duties and no policymaking authority, acting in a quasi-ministerial function. Still, the position was opened to the public, with selection criteria published by the Bureau. *See id*. Parties had opportunities to object to proposals in the public record, and the Bureau, pursuant to its delegated authority, published an order detailing the reasons for its final decision. *See Amendment of Parts 2 and 95 of the Commission's Rules to Create a Wireless Medical Telemetry Service*, Order, 16 FCC Rcd. 4543 (2001).

Similarly, NeuStar cites the cellular system identifier numbers administrators' designation of a central database administrator from among them as an example of a designation not subject to CICA. In that case, the FCC was transitioning that role and handing it off to the private sector. *See Six Organizations Will Assume Responsibility for Cellular SID Administration*, Public Notice, 18 FCC Rcd. 15175 (2003). The CDA was not a separate entity selected by an industry group, as NeuStar characterizes it, (*see* NeuStar Ex Parte Response at 28) but was one of the six SIDA's that the Commission had previously selected after an open and competitive public process.

should be opened up to competitive bidding to serve the public interest, NeuStar does not suggest that doing so would harm the public interest.[53] It instead insinuates that Telcordia hypocritically seeks to subject NeuStar's "lucrative services" to competitive bidding while protecting its own services.[54] Telcordia, however, has not shied away from competitive bidding. Telcordia is not, and the Commission need not be, afraid of competitive bidding procedures.

V. NAPM MUST COMPLY WITH CICA'S COMPETITIVE BIDDING REQUIREMENTS.

The Commission's paramount authority over number portability,[55] subject to CICA's requirements,[56] is without doubt. The question is whether NAPM has the delegated authority unilaterally to extend NeuStar's contract to serve as NPAC Administrator -- and to expand that contract's scope, on a non-transparent, sole-source basis, negotiated entirely behind closed doors, without any statement of requirements – or whether it must or should be required to competitively bid that contract through an open and transparent process. As Telcordia explained fully in its Replies, this is not a close call. CICA's requirements for full and open competition for government contracts apply to the NPAC contract because

- the NAPM LLC is a public instrumentality that, although incorporated as an LLC, has no other business apart from acting as the interim manager and overseer of the NPAC contracts, and it draws its limited authority from government fiat;
- the contract involves the use of public funds collected through the exercise of police power;

[53] *See* NeuStar Ex Parte Response at 22-28.

[54] *Id*. at 22.

[55] 47 U.S.C. § 251(e).

[56] 5 U.S.C. § 105 defines an "executive agency" to include "independent establishment[s]," which in turn includes the FCC.

- the contract is a procurement of a service performed for the government, the implementation of statutory number portability mandates and local telephone competition; and
- Amendments 57, 70 and 72 were modifications beyond the scope of the initial procurement.

Telcordia already presented this analysis in its replies, and now must respond to NeuStar's extraneous and irrelevant analogies and self-serving mischaracterization of the roles of the parties to the contract. NeuStar suggests, for instance, that NAPM, which has no contract with the Commission, is nonetheless a "prime contractor," making NeuStar something like a "subcontractor"; NAPM has made no such claim. Alternatively NeuStar asserts that NAPM has nothing to do with the Commission at all because it is set up as a "private limited-liability company that is composed of private carriers."[57] It casts Telcordia as a "disappointed bidder" although Telcordia has never had the opportunity to bid – and NeuStar has worked assiduously to prevent competitive bidding, including negotiating into Amendment 57 an approximately $30 million annual penalty if NAPM were ever to issue a Request for Information, let alone a Request for Proposals.

NeuStar also reveals its fundamental misunderstanding of CICA with its faulty analysis of the statute and case law. The statute does not contain a definition of the term "procurement." (NeuStar incorrectly states otherwise, claiming that Telcordia seeks to "grossly expand[] the statutory definition of 'procurement.'"[58]) Instead, courts over time have applied a natural or plain meaning of the term to assess whether a contract involves procurement subject to CICA.

[57] NeuStar Ex Parte Response at 11-12.

[58] NeuStar Ex Parte Response at 18.

To further obfuscate the applicability of federal procurement law to the NPAC contract, NeuStar throughout its ex parte cites decisions rendered in different statutory contexts that have no bearing on the applicability of CICA to these facts.[59] NeuStar also distorts the facts, claiming that CICA does not apply to NeuStar, NAPM, or the contracts because they are all "private."

A. The NAPM LLC is a Public Instrumentality.

NeuStar acknowledges that NAPM is subject to the Commission's oversight and control,[60] but argues that this is not sufficient to render NAPM a public instrumentality. NeuStar, attempting to shield itself from competition and the risk of losing the ground it has gained through the sole-source amendments to the NPAC contract, suggests that NAPM could be subject to federal procurement laws only if it were so inextricably intertwined with the Commission as to be a part of the federal government itself.[61]

As Telcordia explained more fully in its replies,[62] the NAPM LLC is a public instrumentality. NAPM exists only to act in the role the Commission has provisionally given to it; it has no function other than to oversee the number portability contract. The Commission has the power through a rulemaking procedure or otherwise to take away the NAPM's ability to function. Telcordia is not challenging the initial interim designation of the NAPM LLC to

[59] *See, e.g., Fed. Reserve Bank v. Metrocentre Improvement Dist*., 657 F.2d 183 (8th Cir. 1981) (holding that a test for whether an entity is a public instrumentality for purposes of taxation is separate from and not dispositive of whether an entity is an instrumentality for purposes of the Federal Tort Claims Act).

[60] See NeuStar Ex Parte Response at 16.

[61] *See id*. at 12 *et seq*.

[62] *See* Reply Comments of Telcordia Technologies, Inc., Docket No. 09-109, at 28 *et seq*. (filed Sept. 29, 2009).

oversee – subject to layers of oversight by the NANC, the Bureau and the Commission[63] – the number portability contract. It is challenging NAPM's extension of its role not just to oversee the administration of the NPAC contract or to make minor modifications, but to make major modifications that embody policy decisions as to what should be covered by the contract, and when and how much competition to permit among potential NPAC Administrators.

To support its claim, NeuStar borrows from federal supremacy case law and Federal Tort Claims Act (FTCA) doctrines addressing when entities fall within the immunity from taxation or liability accorded to the federal government. Different tests apply in different statutory or constitutional contexts to determine whether an entity is a public instrumentality.[64] For tax immunity, courts not only determine whether an entity is an instrumentality, but go further to determine whether that "agency or instrumentality" is "so closely connected to the Government that the two cannot realistically be viewed as separate entities, at least insofar as the activity being taxed is concerned."[65] Whether NAPM could successfully claim that it is immune from state taxation would not be dispositive of whether the contract it oversees should be subject to competitive bidding.

---

[63] Second LNP Order, 12 FCC Rcd. at 12345 ¶ 114 ("In addition, we adopt the NANC's recommendation that it provide ongoing general oversight of number portability administration, including oversight of the individual LLCs, subject to Commission review.")

[64] *See, e.g., Fed. Reserve Bank*, 657 F.2d at 185 n.2 ("Appellees argue that the test recognized in Federal Tort Claims Act cases should be applied here. That test is based on whether the federal government dictates the 'detailed physical performance' of the corporation. *United States v. Orleans*, 425 U.S. 807, 814 (1976); *Logue v. United States*, 412 U.S. 521, 528 (1973). However, because of other policy considerations, the test is different when determining whether an entity is an agency or instrumentality for purposes of the F.T.C.A. than for purposes of taxation. *Federal Land Bank v. Priddy*, 295 U.S. 229, 235 (1935). Therefore we hold the F.T.C.A. test is not dispositive.").

[65] *United States v. New Mexico*, 455 U.S. 720, 735 (1982).

Likewise, FTCA analysis is not dispositive of CICA's applicability to the NPAC contract. The FTCA limits the tort liability of the federal government to acts or omissions of federal government employees and defines "government employees" to exclude any contractor – including those that won their contracts through competitive bidding – with the United States. NeuStar cites United States v. New Orleans, a case in which the court determined that an entity was a "contractor" under the statutory definition and therefore the United States was protected from liability for actions taken by its employees. But *New Orleans* did not address whether that contract itself was subject to federal procurement laws. Taken to its next step, NeuStar's insistence that *New Orleans* applies would mean that NAPM itself is a contractor with the federal government, which it clearly is not. NAPM has no contract with the Commission, but only a limited, interim oversight role with respect to the number portability contract. Whether or not the Commission would be liable for torts committed by NAPM, or even NeuStar, employees has no bearing on whether the contract for number portability administration should be subject to CICA.

NeuStar also relies on *Lewis v. United States*,[66] a case involving the question whether the United States would be liable for the negligence of a Federal Reserve Bank employee under the FTCA. The court explained that although Federal Reserve Banks were considered federal instrumentalities for purposes of immunity from state taxation,[67] they were not federal agencies for purposes of the FTCA.[68] This is an entirely unrelated inquiry.

---

[66] *Lewis v. United States*, 680 F.2d 1239 (9th Cir. 1982).

[67] *See Lewis*, 680 F.2d at 1242 (citing *Fed. Reserve Bank of Boston v. Comm'r of Corps. & Taxation*, 499 F.2d 60 (1st Cir. 1974)).

[68] *Id*. at 1243.

Even if FTCA analysis were dispositive of CICA applicability, these decisions support Telcordia's position that NAPM is a public instrumentality because it is serving a public purpose. The court in *Lewis* noted that there are no "sharp criteria" for determining whether an entity is a federal agency, but among them is "whether the government is involved in the entity's finances" and "whether the mission of the entity furthers the policy of the United States."[69] The court also noted that Federal Reserve Banks are considered federal instrumentalities for purposes of the Service Contract Act, applying an "important government function" test and concluding in that context that the term "Federal government" in that Act should be "liberally construed to effectuate the Act's humanitarian purposes of providing minimum wage and fringe benefit protection to individuals performing contracts with the federal government."[70] With respect to the NPAC contract, NAPM's sole function is to contract for a service on behalf of the Commission in order to implement the Commission's obligation to establish and maintain a long-term number portability database that all carriers must use.

B. The NAPM LLC is Not a Prime Contractor.

NeuStar also attempts to shoehorn the parties to the NPAC contract into a prime-subcontractor relationship and falsely to paint Telcordia as a disappointed bidder.[71] But, as previously set forth, Telcordia never has had an opportunity to bid. This dispute is not a "subcontractor bid protest"; Telcordia is asking the Commission for an opportunity to compete for an NPAC contract, not complaining that it lost. Nor is NAPM LLC a "prime contractor" as NeuStar wishes to suggest.[72] NAPM has no contract of any kind with the FCC. NeuStar thus

[69] *Id*. at 1240-41.

[70] *Id*. at 1243 (citing *Brink's Inc. v. Bd. of Governors*, 466 F. Supp. 116 (D.D.C. 1979)).

[71] *See* NeuStar Ex Parte Response at 19-22.

[72] *See id*. at 21-22.

cannot be a "subcontractor." The Commission instead has authorized NAPM, much like a contracting officer, on an interim basis, to oversee and manage the NPAC contracts.

The line of decisions cited by NeuStar concerning subcontractor bid protests also is not relevant because it relates to the GAO's jurisdiction to hear appeals from disappointed potential subcontractors.[73] The Commission need not consider whether it has jurisdiction to entertain this dispute. It has paramount authority and responsibility to the industry and consumers over implementation of number portability, and the ability to designate numbering administrators under Section 251(e)(1). In erroneously citing this line of cases about agency jurisdiction, NeuStar once again attempts to complicate this dispute and evade regulatory oversight.

C. The NPAC Contract Involves the Use of Public Funds.

NeuStar also tries to insulate the contract from competition by labeling it "private" and the regulatory fee payments as "fees that the *private* carriers pay NeuStar for its services under the *private* contracts."[74] It additionally mischaracterizes the mechanism by which this payment is made, as if there is a direct "exchange" of "the payment of money by the *carriers*" for "administration of and access to the local number portability database."[75] NeuStar maintains that

[73] *See US West Commc'ns Serv., Inc. v. United States*, 940 F.2d 622, 628 (Fed. Cir. 1991) (explaining that "past practice [] precluded subcontractor actions before the board" because "the then-existing procedures of the board were suitable for considering federal agency procurements"); *In re St. Mary's Hospital and Medical Center of San Francisco*, 70 Comp. Gen. 579, B-243061 (1991) (finding the procurement subject to GAO's bid protest jurisdiction because the contractor was a "conduit" for the government and therefore the procurement was subject to CICA requirements); *In re Compugen, Ltd*., 1995 U.S. Comp. Gen. LEXIS 583 (1995) (GAO did not take jurisdiction over a challenge to sole-source subcontract award by a losing bidder); *In re Alatech Healthcare, LLC*, 2009 U.S. Comp. Gen. LEXIS 40, *5 (2009) (GAO declined to consider protest of an award of a subcontract, explaining that it no longer asserted jurisdiction over certain procurements that were made by a prime contractor for the government even if "federal procurement laws and regulations otherwise would apply").

[74] NeuStar Ex Parte Response at 15 (emphasis added).

[75] *Id*. at 18.

these mandatory number portability fees are "fees that NeuStar charges for its *private* services."[76] But NeuStar identifies no other so-called private contract, and Telcordia knows of none, that is backed by federal government police power and enforcement authority.

NeuStar cannot dispute and therefore must concede "the simple fact that carriers are required by law to participate in the NPAC arrangement."[77] Federal law and regulation require carriers to participate in and pay for number portability database administration based on an FCC-established formula. As NeuStar explains, the "Commission establishes the formula that distributes the burden of the fees among carriers."[78] Carriers do not pay NeuStar in proportion to their use of the database. The amount of the carrier's payment is ultimately set by the assessment formula in the Commission's rules, which are then merely mirrored in the contract and from which the NeuStar contracts may not deviate.[79] Carriers who fail to pay these mandatory fees risk Commission enforcement proceedings, including forfeitures and fines.[80] This enforcement risk applies even to carriers that never port a single number or function as an "n-1" carrier, and thus never use NeuStar's services. Procurements such as this involving the expenditure of public funds through the use of the police power are subject to federal procurement laws.[81]

---

[76] *Id*.

[77] NeuStar Ex Parte Response at 16.

[78] *Id*. at 16 n.63.

[79] 47 C.F.R. § 52.32.

[80] *See, e.g., In re Telrite Corp. Apparent Liability for Forfeiture*, Notice of Apparent Liability for Forfeiture and Order, 23 FCC Rcd. 7231, 7237 ¶ 12 & n.42 (2008).

[81] *See* Telcordia Reply Comments at 28-30 (citing *Motor Coach Indus., Inc. v. Dole*, 725 F.2d 958, 961-62 (4th Cir. 1983)).

D. The NPAC Contract is a Procurement for Government Services.

As Telcordia explained in its replies, the NPAC database administration is a procurement to serve the public purpose of local number portability and local telephone competition.[82] NeuStar suggests that the NPAC contract does not involve a "procurement" at all, but cites cases involving procurements. As noted above, CICA does not define "procurement," but courts have applied a plain meaning to that term. Under those cases – which NeuStar cites -- the NPAC contract is a procurement subject to federal procurement laws.

NeuStar contends, citing *Rapides Regional Medical Center*, that CICA's requirements to apply to government decisions only when they "involve the government's paying money or conferring other benefits in return for the acquisition or use of private property or services."[83] In that case, two hospitals, one private, one operated by the Department of Veterans Affairs (VA), entered into an agreement to acquire and share a piece of equipment. The VA hospital bought the equipment, but the private hospital donated half the cost. A different medical center that had previously contracted with the VA for use of its machine challenged the sharing agreement as violating CICA. The court disagreed, stating that an agreement over future access to government-owned property was not a procurement. There was no disagreement, however, that the VA's initial purchase of the equipment from the manufacturer *was a procurement* that had been conducted using competitive procurement procedures, and that procurement was not at issue in the case.[84]

---

[82] *See id*. at 30.

[83] *Rapides Reg'l Med. Ctr. v. Sec'y, Dep't of Veteran's Affairs*, 974 F.2d 565, 574 (5th Cir. 1991).

[84] *See id*. at 572.

NeuStar then asserts, relying on an incomplete quotation from *Corel v. United States*,[85] that CICA does not apply "to government decisions which do not involve the actual purchase of a good or service" for use by the government. The rest of the sentence, however, provides "nor does CICA apply when the government is merely purchasing a good or service to which the government already possesses a right." In that case, the government had awarded an "indefinite quantity contract" to a retailer. That contract was not at issue. Instead, a software manufacturer challenged the Department of Labor's decision to standardize its software and adopt software manufactured by Microsoft, which it would then purchase from the retailer. The software purchase unquestionably constituted *a procurement.* The decision instead turned on whether that procurement was conducted pursuant to a different procurement statute, rendering CICA inapplicable under CICA's savings clause.[86] In fact, the Department of Labor conducted its "procurement" under the Federal Acquisition Streamlining Act (FASA). FASA specifically exempts indefinite delivery contracts from competition.[87] Thus, the court held that because FASA expressly authorized DOL's procurement procedures, CICA's savings clause deferring to other statutes authorizing conflicting procurement procedures rendered CICA inapplicable.[88] Here, however, NeuStar does not suggest that some other federal procurement laws govern in lieu of CICA. Its point is more extreme: it insists that none do.

NeuStar also relies on *Grigsby Brandford & Co., Inc. v. United States* in arguing that CICA is inapplicable. The *Grigsby* court held that CICA did not govern the original designation

---

[85] 165 F. Supp. 2d 12, 24 (D.D.C. 2001).

[86] *See id.* at 31-32.

[87] *See id*. at 31 ("FASA specifically provides that, when an agency issues a task or delivery order under an indefinite delivery contract, the agency is not required to conduct a 'competition (or a waiver of competition approved in accordance with *section 253(f)* of this title) that is separate and apart from that used for entering into the contract.'" (citing 41 U.S.C.A. § 253j(a)(2))).

[88] *See id*. at 194 (citing 41 U.S.C. § 253(a)(1)).

of a Designated Bonding Authority (DBA) for the Historically Black Colleges and Universities Capital Financing Program because the designation was not a procurement. Instead, the DBA designation was the "creation of a status rather than the procurement of goods or services."[89] The FCC's provisional designation of NAPM as the entity to oversee the NPAC contract is the analog to the DBA designation here, not the award of the contract to NeuStar. Telcordia does not contend that the interim designation of the NAPM LLC in its oversight role was itself a procurement. Moreover, *Grigsby* relies on a (non-CICA) case holding that the Treasury Department's selection of a national bank to serve as a financial agent for a new system of cash concentration and reporting was not a procurement within the meaning of the Brooks Act. Instead, designating a financial agent is akin to appointing federal employees, not a procurement. These cases involve the "conferral of status" rather than the procurement of goods or services. NeuStar's role as the monopoly vendor of NPAC database administration services is different. NeuStar performs a service for the government and receives public funds – i.e., funds collected by law through the exercise of the police power -- to do so.

E. The Contract Modifications are Outside the Scope of the Original Procurement.

The modifications to the NPAC database administration contract changed the contract so dramatically in duration and scope as to circumvent CICA's requirement of competition. There can be no doubt, and NeuStar does not dispute, that modifications outside the scope of the original contract fall under CICA's statutory competition requirement.[90] CICA sets no standard for determining when modification of an existing contract requires a new competition or falls

[89] *Grigsby v. United States*, 869 F. Supp. 984, 999 (D.D.C. 1994). Further, *Grigsby* is inapplicable because there, unlike in this case, another statute governed the selection of a DBA, bringing the selection within the CICA's savings clause.

[90] 41 U.S.C. § 253 (a)(1)(A).

within the scope of the original competitive procurement.[91] Courts, however, have determined that a modification that "materially departs from the scope of the original procurement violates CICA by preventing potential bidders from participating or competing for what should be a new procurement."[92]

The initial RFPs for NPAC database administration contained provisions regarding "Future Considerations," providing that "[t]he future of number portability, such as the number of service providers and possible expansion to geographic and service portability, and number administration are not known at this time. The SMS platform should not preclude future expansion to adapt to additional needs as they arise."[93] But the RFPs also provided a bulleted list of seven specific examples of the types of future considerations that bidders should consider in preparing their bids. Those considerations included expanding the database to CMRS providers and to other geographic regions, permitting geographic number portability, pooled NXXs, and overlay NXXs, and expanding to include resellers. Nothing in this list would put industry on notice that the contract might be modified to expand into VoIP or the information services space.

Moreover, the initial RFPs directed bidders to submit proposals "provid[ing] both a three year and five year view."[94] The "Future Considerations" section contained no provision about extending the duration of the contract. In any event, the request for a three- or five-year view certainly suggested a three- or five-year term for the contract. Nothing in the RFPs put vendors

---

[91] *AT&T Commc'ns, Inc. v. Wiltel Inc.*, 1 F.3d 1201 (Fed. Cir. 1993).

[92] *CWT v. United States*, 78 Fed. Cl. 486, 494 (Ct. Fed. Cl. 2007) (citing *CESC Plaza Ltd. P'ship v. United States*, 52 Fed. Cl. 91, 93 (2002)). In *CWT*, the court rejected a protest claiming that a delay to the start date and price modifications constituted cardinal changes requiring a new competitive bid. The court found that the solicitation did not specify a start date and that the price modifications were contemplated by the solicitation which authorized price negotiations to deal with changes in ticket volume requirements and technology.

[93] West Coast Portability Services, LLC's Request for Proposal § 13 (attached as Attachment 1).

[94] *See, e.g.*, Illinois Request for Proposal at 9 (attached as Attachment 2).

on notice that the contract might be open-ended, much less indefinite – and certainly not that the contract could be modified to become a *de facto* monopoly contract lasting for at least seventeen years. Instead, the RFPs proposed finite time periods, and the most that vendors reasonably could have anticipated in pricing their bids (and recovering their initial costs) was that the contract might last up to five years.

Through Amendments 57, 70 and 72, among others, however, NAPM and NeuStar have extended the duration of the contract to run at least *seventeen* years; changed the scope of the contract by adding URI fields for IP routing, picture messaging and SMS, permitted NeuStar to use the NPAC database to supply ENUM services; and adopted substantial changes in pricing structures by moving from a per-transaction structure which would permit immediate substitution to a new entrant to a quasi-fixed-price contract that essentially precludes competitive entry until the expiration of the fixed price arrangement. As Telcordia set forth in its replies, these cardinal changes to term, scope and pricing structure constitute a new procurement that should be subject to competition.[95]

NeuStar makes a last-ditch effort to claim that the modifications somehow fit within the scope of the original contract. NeuStar further argues that because the original contract contained a "changes clause" encompassing modifications, subsequent modifications need not be rebid.[96] The Master Agreement provided that at any time during the Agreement, NAPM could request "new or additional services" and that NeuStar could propose additional services.[97] The

[95] *See* Telcordia Reply Comments at 34-37. NeuStar's arguments about the economic rationality and purported benefits and cost savings to the industry are not only wrong as Telcordia has previously demonstrated but are beside the point. A post hoc rationalization for violations of CICA competition requirements cannot exempt the contract from competitive bidding.

[96] *See* NeuStar Ex Parte Response at 29.

[97] Master Agreement Arts. 13.1-13.2.

original RFP set forth what vendors would have understood "new or additional services" to include. As described above, the original RFPs provided a three- or five-year contract term, and certain specific services and possible future services. As discussed above, the subsequent amendments, however, have materially departed from what any bidders at the time could have anticipated.

The cases NeuStar cites to support its argument that these fundamental changes to the contract are within the scope of the original agreement are unavailing, and are factually distinct because they involve changes that were less substantial or could reasonably have been anticipated by bidders.[98] Indeed, *Global Computer Enterprises, Inc. v. United States*,[99] a recent and lengthy opinion on which NeuStar relies, found that modifications exceeded the scope of the original contract and violated CICA. As the *GCE* court recognized, to determine whether a modification falls within the competition requirement of CICA, a court must focus on the "scope of the entire original procurement in comparison to the scope of the contract as modified."[100]

---

[98] *See AT&T Commc'ns* , 1 F.3d at 1207. For example, in *AT&T Commc'ns*, the court was presented with a single type of change – adoption of new technologies within a contract containing a requirement for a Service Improvements Clause and an annual forecast of new technologies in a comprehensive telecommunications contract. Duration, pricing, and other terms remained constant, but the service provided under the contract changed to the latest commercially available technology. Similarly, in *CWT*, the challenge related merely to a "delay in commencement" of the contract by a little more than two years and price modifications related to an "equitable adjustment clause" already in the contract. *CWT*, 78 Fed. Cl. at 487 n.1. NeuStar also cites *HDM Corp. v. United States*, 69 Fed. Cl. 243 (Ct. Fed. Cl. 2005), a case in the modification at issue did not significantly change the performance period of the contract. The court explained that "[a]dditional time spent on performance of a contract is within the scope of the contract when it is due to problems with the completion of performance." *Id*. at 256 (citing *Northrop Grumman Corp. v. United States*, 50 Fed. Cl. 443, 466 (2001)). In addition, with respect to other challenged changes, the original contract contained "significant language" alerting prospective bidders that the methods of meeting the contract's objectives would likely change and evolve.

[99] *GCE*, 88 Fed. Cl. 350, 381.

[100] *Id*. at 426.

Although there is "no exact formula" for determining whether changes are outside the scope of the original procurement, "[e]vidence of a material difference between the modification and the original contract is found by examining any changes in the type of work, performance period, and costs between the contract as awarded and as modified."[101]

In *GCE*, much like the present situation, an IT services contract was expanded to include financial IT support. The court found that the original task order did not contemplate an unlimited expansion of computer systems and agreed with the complainant that the Government should not be allowed "to pour whatever IT support work it desires into the SETS II task order scope, regardless of the nature of the work."[102] This is precisely what NeuStar is attempting to preserve for itself – the ability to pour whatever fields and data into the NPAC that it possibly can to make its administration of the database more, to borrow NeuStar's own term, "lucrative."

Further, just as NeuStar has been hard-pressed to justify how the expansion of the database to encompass more IP fields is "necessary" under Commission rules for number portability,[103] the *GCE* court found that certain modifications to the contract to include audit-

---

[101] *Id*. at 427 (quoting *MCI Telecommc'ns Corp*., B-276659.2, 1997 WL 602194, at *6 (Comp. Gen. Sept. 29, 1997).

[102] *Id*. at 430.

[103] *See, e.g., Telcordia Request that NANC Resolve Dispute Concerning Necessity of Adding Certain URI Codes for the Completion of Telephone Calls* (May 26, 2009), http://nanc-chair.org/docs/mtg_docs/Telcordia_Dispute_Resolution_Request_Final.pdf; *NeuStar Opposition to Telcordia's Request that NANC Resolve Dispute Concerning Necessity of Adding Certain URI Codes for the Completion of Telephone Calls* (Aug. 14, 2009), http://nanc-chair.org/docs/mtg_docs/NeuStar_Response.pdf; *Telcordia Reply in Support of Telcordia Request that NANC Resolve Dispute Concerning Necessity of Adding Certain URI Codes for the Completion of Telephone Calls* (Aug. 31, 2009), http://nanc-chair.org/docs/mtg_docs/Telcordia_Response_August_31_2009.pdf; *see also* 47 C.F.R. § 52.25(f). NeuStar circumvents any discussion of the regulatory obligation under Section 52.25(f) of the Commission's rules that the NANC make a determination, in the first instance, whether changes to the database are necessary for number portability. NeuStar in its ex parte conflates its argument that changes are within the scope of the original procurement with the notion that the change management processes governing changes to the database architecture –

supporting federal financial management systems exceeded its original scope because they did not support the Coast Guard's stated strategic missions in accordance with the task order.[104] Moreover, the change orders and task orders improperly extended the scope of the underlying contract beyond its original ordering period, also a substantial modification found to violate the CICA.[105]

The *GCE* court, citing the Comptroller General's decision in *CPT*, recognized that the proper remedy for failing to competitively bid is to re-bid the contract, not to allow the contract to continue. It found that the petitioner's exclusion from the competitive bidding process was sufficient harm alone to warrant a permanent injunction.[106] "No adequate remedy exists to make up for GCE's potential loss of business. Accordingly, GCE has been irreparably injured because it was excluded from competing for audit-supporting federal financial management systems services due to the Coast Guard's violation of the CICA."[107] The court therefore directed the Coast Guard to procure these services "in accordance with the law and in a manner that preserves the integrity of the procurement process."[108] Evaluating the public interest in the injunction, the court wrote: "Healthy competition ensures that the costs to the taxpayer will be minimized. The

---

another way that NeuStar is subject to oversight – somehow put all potential bidders on notice that the NPAC contract could encompass changes to the NPAC data fields beyond what is necessary for number portability as well as an extension of the term of the contract for more than a decade. *See* NeuStar Ex Parte Response at 33-34.

[104] *GCE*, 88 Fed. Cl. at 432. The court compared the task order to that at issue in *CPT Corp*., discussed by Telcordia in its replies, *see* Telcordia Reply Comments at 35 (discussing *In re CPT Corp*., 1984 U.S. Comp. Gen. LEXIS 1037 (Comp. Gen. June 7, 1984)), and concluded that adding financial management systems under a task order that called for "computer systems" was a modification beyond the scope of the original task order. *See GCE*, 88 Fed. Cl. at 436.

[105] *See GCE*, 88 Fed. Cl. at 444-45.

[106] *See GCE*, 88 Fed. Cl. at 452 n.122.

[107] *GCE*, 88 Fed. Cl. at 453.

[108] *Id*. at 461.

public interest is clearly served when suppliers engage in fair and robust competition for government contracts, and granting injunctive relief in this case ensures that public confidence and competition in the federal procurement process will be preserved."[109] Those principles have equal force and applicability here. The contract must be rescinded and immediately re-let for competitive bidding.

CONCLUSION

This proceeding addresses a straightforward problem with a simple solution. NeuStar, for too long, has been allowed to operate as number portability Administrator without having to pass the market test of competitive bidding. Number portability administration is no less of a Commission program NANPA administration and number pooling administration. Yet unlike those other programs, there have been no competitive bids since 1997, and NAPM has continually extended and expanded the NPAC contracts without FCC authorization or approval. Moreover, unlike NANPA administration and number pooling, NAPM, not the Commission, makes the decision whether to execute contract amendments – and NAPM does not even give the Commission an opportunity to review its actions before they become effective. The result has been thirteen years without competitive bids and chronically overpriced, *de facto* exclusive number portability administration contracts that harm the public interest in honest, open, and fair competition.

This Commission must not allow this anticompetitive state of affairs as a *fait accompli.* It has full authority to alter course and reinstate competitive bidding and open, transparent accountability. Under the current contract, industry and consumers will pay an estimated $2.8 billion between 2009 and the end of 2015 to NeuStar for NPAC administration services. If, like

[109] *Id*. (internal citations and quotations omitted).

Amendment 57, that proves to be at least 20% too much, industry and consumers will have been overcharged by at least $500-$600 million. The only way the Commission can assure itself and the public that it has gotten the best terms possible for number portability administration – and that the public is not being forced to pay too much – is to put number portability administration out for competitive bid. As the President directed, "[t]he Federal Government has an overriding obligation to American taxpayers. It should perform its functions efficiently and effectively while ensuring that its actions result in the best value for the taxpayers."[110] That is as true for the Commission with respect to number portability administration as it is for any other arm of the federal government. We urge the Commission to act now to reinstate competitive bidding and bring open, transparent accountability to its number portability program.

Respectfully submitted,

/s/ John T. Nakahata
John T. Nakahata
Linda McReynolds
Madeleine V. Findley
WILTSHIRE & GRANNIS LLP
1200 18th Street NW
Washington, DC 20036
(202) 730-1320

Counsel for Telcordia Technologies, Inc.

[110] Memorandum for the Heads of Executive Departments and Agencies, 74 Fed. Reg. 9755, 9755 (Mar. 4, 2009).

Attachment 1

Section 1: General Information

1.1. Introduction

1.1.1. Purpose of This Request For Proposal (RFP)

This Request For Proposal is being issued by the West Coast Portability Services, LLC (WCPS) to invite respondents (Primary Vendors) to submit responses presenting a complete "turnkey" database solution, related firm pricing proposal and commitment to provide a Number Portability Administration Center (NPAC) and Service Management System (SMS). WCPS was formed by certain of the participating carrier members of the California Local Number Portability Task Force (CLNPTF) with the guidance of the California Public Utilities Commission (CPUC) (D.96-08-041) in order to manage the database Local Number Portability (LNP) procurement in accordance with this RFP. Initially, WCPS expects the NPAC/SMS will support the statewide implementation of LNP in California with possible expansion to other states.

WCPS'S DECISION IN ISSUING THIS RFP DOES NOT MEAN THAT CALIFORNIA IS OPTING OUT OF ITS NANC-DESIGNATED REGIONAL DATABASE. THIS "OPT-OUT" DECISION RESTS WITH THE CPUC AND FCC (SEE FCC ORDER 96-286 ADOPTED IN DOCKET 95-116 ON JUNE 27, 1996 AT PARAGRAPH 96). WCPS BELIEVES THAT A NPAC/SMS VENDOR MUST BE SELECTED IN 1996 IN ORDER TO MEET FCC TIMELINES FOR METROPOLITAN STATISTICAL AREAS (MSAs) SCHEDULED FOR PERMANENT LNP IN 1997. WCPS ALSO BELIEVES THAT PROCEEDING WITH ITS RFP NOW WILL SUPPORT CALIFORNIA AS EITHER A STATE PARTICIPATING IN A REGIONAL NPAC/SMS, A CENTER OF A REGIONAL NPAC/SMS INCLUDING OTHER STATES, OR IN A STAND-ALONE "OPT-OUT" SCENARIO.

Primary Vendor responses must be based upon the specifications provided in this RFP and should contain detailed information on degree of compliance with requirements, pricing and availability, as specified herein.

The Evaluation/Procurement (E/P) Team, which will evaluate all responses to this RFP, is made up of one voting representative from each of the members in good standing of WCPS. WCPS's E/P Team may solicit the counsel of the CPUC Staff, and any other industry/company experts to facilitate this evaluation (including but not limited to risk management expertise, legal, procurement, and/or relevant matters of a technical nature). The E/P Team may involve other participants in the CLNPTF in the review process on a

non-voting basis. WCPS's E/P Team will evaluate all proposals from a total network and operations perspective to ensure integration with existing network and operating procedures. Proposals will also be assessed on their ability to evolve, as necessary, from serving a limited geographic area into a regional and/or nationwide service, with minimal obsolescence of existing investment (See Section 1.5. Evaluation/Procurement of Proposals).

1.1.2. RFP Information and Usage Restrictions

Primary Vendors and their employees, consultants, agents, etc., shall utilize this RFP and any other information furnished relating to this RFP solely for the purpose of responding to this RFP. All such documents and information you receive shall remain the property of WCPS, shall be kept confidential and shall be returned to WCPS upon request. Reproduction of any part of this RFP is authorized only for the preparation of a formal response, as Primary Vendor, or as a Sub-Contractor to a Primary Vendor to this RFP. Primary Vendors shall not disclose this RFP to any employees, agents or independent contractors who do not have a "need to know" or to any third party working with or for you without the prior written consent of WCPS's E/P Team, except of course, that a Sub-Contractor may be provided a copy of the RFP for preparation of its portion of the Primary Vendor's response under this RFP.

1.1.3. Primary Vendor's Information

Do not submit any proprietary or confidential information or mark it as such. Information furnished by you to the E/P Team pursuant to this RFP shall not be considered by you to be confidential or proprietary. In no event will the E/P Team consider or hold any information contained in your proposal proprietary or confidential, except for the pricing information specified in Section 1.4.3.2.

1.1.4. Background of Local Number Portability in California

1.1.4.1. History of LNP Activities in California

As part of CPUC rulemaking on local competition (D.95-07-054), the CLNPTF was formed in May 1995, consisting of various telecommunications industry organizations, with a mission to evaluate, recommend, and ultimately implement a technically and economically feasible solution for service provider number portability meeting the needs of California consumers and carriers in a competitively neutral manner.

The CLNPTF submitted a progress report to the CPUC on February 29, 1996. Additional work and proposed implementation schedules confirmed the

requirement for the issuance of an RFP and the selection of a database administrator for the NPAC/SMS.

The implementation timing of permanent LNP was subsequently addressed in FCC Order 96-286. According to that schedule, phased implementation in the 100 largest MSAs must begin no later than October 1, 1997 with deployment complete by December 31, 1998. Thirteen MSAs in California are included in the FCC's list.

On July 3, 1996, the Service Management System Subcommittee of the CLNPTF submitted a report to the CPUC outlining the requirement for a state NPAC/SMS to facilitate permanent LNP, and the need for an RFP process to achieve that end. The CPUC subsequently ordered the CLNPTF to proceed in the selection of a vendor in order to meet the FCC's implementation schedule.

WCPS has been established as the legal entity empowered to issue, manage, and contract for the procurement in accordance with this RFP.

Consistent with the FCC's timetable, it is the intention of WCPS to select a Primary Vendor to manage and establish the NPAC/SMS platform no later than December 31, 1996, start NPAC/SMS testing by second quarter of 1997, with targeted full functional operability in the third quarter of 1997 (including the porting of live telephone numbers).

1.1.4.2. Impact of State and Federal Regulation and/or Legislation on this Procurement

This RFP is being issued by WCPS whose members are a group of service providers who currently provide or intend to provide facilities-based local exchange services in the state of California through the porting of local telephone numbers. LNP implementation is subject to direct regulatory oversight by the CPUC and FCC. However, Primary Vendors should be aware that in addition to state and federal regulatory oversight, the federal government, through congressional legislation, other actions and/or mandates, may establish policies for local competition which may affect the operation of the California NPAC/SMS platform. The NPAC/SMS requirements are subject to change pending publication of North American Numbering Committee (NANC) standards or any other applicable law or regulation.

Moreover, it is the express and stated intent of WCPS to: (1) comply with any order or other directive concerning LNP issued by the CPUC or the FCC, including, but not limited to, any directive to expand, reduce, merge, consolidate,

dissolve and terminate, or otherwise modify this RFP; and/or (2) supervise and oversee the Primary Vendor and any Sub-contractor or vendor to ensure compliance with any such order or other legal/regulatory directive.

1.2. Description of LNP Environment

1.2.1. LNP Architecture

Pursuant to FCC Order 96-286 and CPUC Decision 96-08-028, WCPS will implement the L~~RN~~ocation Routing Number (LRN) architecture to enable the correct routing of calls in the LNP environment. Although these are final decisions, some parties have requested reconsideration of the FCC order and modification of the CPUC Decision, which may allow further consideration of additional LNP architectures.

1.2.2. Functions of the Service Management System (SMS)

The SMS is a hardware and software platform which contains the database of information required to effect the porting of telephone numbers in California, with possible expansion to other states. In general, the SMS receives information from both the old (confirmation) and new service providers (customer information, including the new Location Routing Number), validates the information received, and downloads the new routing information when an "activate" message is received indicating that the customer has been physically connected to the new service provider's network. The SMS also contains a record of all ported numbers and a history file of all transactions relating to the porting of a number. The SMS shall provide the ability to retransmit LNP information to service providers under certain conditions. The SMS is not involved in real time call processing, because this function resides solely in the respective networks of the underlying carriers.

The NPAC/SMS interfaces with service providers via their Service Order Activation (SOA) system and local SMS. The NPAC/SMS Interoperable Interface Specification (IIS) shall define the interface between the NPAC/SMS and the SOA system. The IIS also defines the interface between the NPAC/SMS and the local SMS. The NPAC/SMS Functional Requirements Specification (FRS) shall define functional and operational requirements for the NPAC/SMS.

1.2.3. Management and Integration Role of Primary Vendor's Number Portability Administration Center/NPAC Function

The NPAC shall provide management, administration, oversight for, and integration of, the data center operations, hardware and software development, and all maintenance related functions. It shall have responsibility for achieving performance standards

established by the industry, for providing user and technical support services, for providing off-line testing with service providers' systems and training for industry participants on an ongoing day-to-day basis.

1.3. Eligibility to Submit Proposals

1.3.1. Qualification of Primary Vendor Bidders

The E/P Team requests that Primary Vendors that plan to bid on the RFP present Qualification Applications (these must list the key business terms and conditions contained in Section 16) by no later than noon Pacific Daylights Savings Time on September 30, 1996 to WCPS concerning: 1) financial responsibility and stability (capability to perform the contract); 2) experience relevant to performance of the contract; 3) neutrality [address the vendor's compliance with the requirement that the system administrator (Primary Vendor) be a neutral third party], and disclose the identity and corporate affiliation of software and hardware Sub-Contractor(s), if any; disclose any contractual relationships, arrangements or other factors that would enhance or impair its ability to perform the administrative (Primary Vendor) function as a neutral third party, 4) indicate Primary Vendor's acceptance and compliance with the key business terms and conditions specified below in Section 1.3.2., 5) provide a list of sub-contractors, if any, for review and approval, and 6) indicate its commitment and ability to adopt and comply with the RFP's delivery schedule included in the cover letter to this RFP.

WCPS's E/P Team will evaluate the Qualification submissions and require at least a simple majority vote to accept or reject each submission based upon financial responsibility, relevant experience, neutrality, acceptance of key business terms and conditions, and acceptance/compliance with the delivery schedule (See Section 1.5, Evaluation/Procurement of Proposals).

WCPS will notify Primary Vendors concerning whether their submission was accepted or rejected, and identify why a submission was rejected, but only if the reason is failure to meet the neutrality criteria. Unsuccessful proposals (on the basis of neutrality as defined in Section 1.3.4. following) may be revised and submitted again, within a period of time as specified by WCPS, in its notice to the Primary Vendor. This method will allow WCPS to address potentially problematic neutrality issues, and allow vendors to correct them, before the time and expense of a full response to the RFP is undertaken. Further, it will allow members of WCPS to be assured that any of the actual bidders of the RFP will be neutral.

1.3.1.1. Financial Responsibility

RFP Qualification Applications must include a concise description of the financial condition of the Primary Vendor and Sub-Contractors, if any. Submissions must include the most recent audited financial statements and annual report for the previous three years of the Primary Vendor and the Sub-Contractors, if any. Submissions must include all characteristics of Primary Vendors financial strength to demonstrate support that it can perform under a multi-year business contract to be awarded under this RFP.

1.3.1.2. Experience Relevant to Performance of the Contract

RFP Qualification Applications must include a concise description of the telecommunications experience of the Primary Vendor and Sub-Contractors, if any, including such items as products and services offered, customers served, successful performance of the functional/technical skills required by this RFP on activities performed for other customers, and customer benefits that resulted from such successful performance.

RFP Qualification Applications must include a concise description of the principal business of the Primary Vendor and Sub-Contractors, if any, including such items as company background, characteristics of business strength, accomplishments and capabilities which demonstrate a strong foundation for managing and operating the NPAC.

1.3.1.3. Neutrality

The Primary Vendor must demonstrate an understanding, willingness, and ability to implement policies and procedures that will ensure evenhanded treatment of all carriers, and certification that the Primary Vendor and Sub-Contractor(s), if any, shall comply with the neutrality provisions of Section 1.3.4. of this RFP, at all times.

1.3.2. Primary Vendor's Acceptance Of Key Business Terms And Conditions

Each Primary Vendor submitting a Qualification application to WCPS must list the following key business terms and conditions and indicate its full agreement to these key business terms and conditions, as a pre-condition to being considered for a contract award as a Primary Vendor, by placing an "X" in the space next to each item listed. The key business terms and conditions are contained in Section 16 of this RFP. These terms and conditions are expected to form a part of the Master and Service Agreements to be executed with the Primary Vendor selected under this RFP, if any, and may not represent a full and complete listing of all contractual terms and conditions incorporated into those agreements.

1.3.3. Primary Vendor

The NPAC/SMS Master Contract and Service Agreements to be awarded as contemplated by this RFP will be awarded to a single Primary Vendor who shall be completely and totally responsible for providing a total "turnkey" solution encompassing the NPAC functionality and the SMS platform (both hardware and software). The Primary Vendor shall be responsible for all NPAC administration duties and system performance/adherence in accordance with the requirements of this RFP and the expectations of WCPS. The Primary Vendor shall be the single point of contact between WCPS and the NPAC/SMS Vendor(s). The Primary Vendor shall be required to submit a comprehensive response to this RFP to provide all elements of the solution. At its option, the Primary Vendor may use its own resources exclusively or engage the services of Sub-Contractors to provide one or more elements of the SMS platform (i.e., hardware, software, etc.), or other elements of the total "turnkey" solution. However, all such arrangements and/or affiliations entered into by the Primary Vendor to provide the total NPAC/SMS solution must be clearly described in the Primary Vendor's Qualification Application Submission (Section 1.4.1.), and subsequently, in the Qualified Primary Vendor's RFP response.

1.3.4. Eligibility to bid on the RFP (Neutrality)

In order to prevent a real conflict of interest, and comply with the CPUC's Order D.95-07-054, the Primary Vendor/System Administrator must be a neutral third party that has no financial or market interest in providing local exchange services within the United States of America.

To prevent such a conflict of interest, the Primary Vendor/System Administrator "NPAC" function ***will not*** be awarded to:

1.) any entity with a ***direct material financial interest*** in the ***United States portion*** of the North American Numbering Plan (NANP), and number assignments pursuant to such Plan, including (but not limited to) telecommunications carriers;

2.) any entity with a ***direct material financial interest*** in manufacturing telecommunications network equipment;

3.) any entity affiliated in other than a *de minimus* way with any entity described in 1.) or 2.) above, or;

4.) any entity involved in a contractual relationship or other arrangement that would impair the entity's ability to administer numbers fairly under the NANP and in accordance with the procedural delivery schedule established by WCPS and set forth in this RFP, (See cover letter to this RFP).

The technical requirements for SMS hardware and software will be defined in this RFP. It is possible for a company that is precluded from being a Primary Vendor/Systems Administrator to act as an SMS Sub-Contractor (hardware/software provider) to a neutral third party Primary Vendor, in responding to this RFP.

A Primary Vendor's response to this RFP must fully disclose the corporate identity or affiliation of its vendor Sub-Contractor(s), if any. ***Failure to adequately do so will be a basis on which to disqualify the Primary Vendor's response.***

1.3.5. Sub-Contractors

Responses to this RFP shall clearly state the roles and responsibilities of any and all Sub-Contractors which are providing parts of the total "turnkey" solution under the direction of the Primary Vendor. Notwithstanding anything to the contrary in this RFP or any Primary Vendor's response hereto, the Primary Vendor selected by WCPS shall remain responsible for the performance of its Sub-Contractors.

1.4. Preparation of Primary Vendor's Response to this RFP

1.4.1. Qualification Application Submission

All Primary Vendors wishing to submit proposals in response to this RFP, complete in every respect, must first submit their Qualification Application to the following members of WCPS's RFP E/P Team, at the addresses provided in the table below, to establish their eligibility to respond to this RFP:

Company	*Name and Address*	*Voice and Fax Numbers*	*Num of Copies*
AT&T	John Meyer AT&T 795 Folsom Rm. 230 San Francisco, CA 94107	*voice:* 415.442.2164 *fax:* 415.442.2190	2

MCI Metro	Steve Addicks MCI Metro 2250 Lakeside Blvd Richardson, TX 75082	*voice:* ~~214.498.5062~~ ~~*fax:*~~ ~~214~~972.498.5062 *fax:* 972.918.1499	1
TCG	Dwight Hakim Teleport Communications Group Two Teleport Drive, 2nd Floor Staten Island, NY 10311-1004	*voice:* 718.355.2623 *fax:* 718.355.4596	1
Time Warner	Jeff Sambdman Time Warner Communications 5680 Greenwood Plaza Blvd. Suite 150 Englewood, CO 80111	*voice:* 303.705.4641 *fax:* 303.705.1874	1
GTE	Bob Angevine GTE Tel ~~Ops HQ-W03B16~~ ~~700 Hidden Ridge~~ephone Operations 700 Hidden Ridge HQW03B16 Irving, TX 75038	*voice:* ~~214.718.4389~~ ~~*fax:*~~ ~~214.718.3606~~972.718.3606 *fax:* 972.718.4389	1
Pacific Bell	Sandra Cheung Pacific Bell 2600 Camino Ramon 2s151 San Ramon, CA 94583	*voice:* 510.823.9562 *fax:* 510.867.3817	1
MFS	Bob Munoz MFS Communications 185 Berry St Suite 5100 San Francisco, CA 94107	*voice:* 415.882.2320 *fax:* 415.957.3758	1
Cox	Dr. Francis Collins CCL Corp. 176 Rangeley Road Chestnut Hill, MA 02167	*voice:* 617.277.8585 *fax:* 617.277.2132	1

A cover letter should be provided which includes both the name, phone number, and FAX number of the individual within the Primary Vendor's organization which can be contacted in case any questions arise during the Evaluation/Procurement phase of its submissions. A Primary Vendor's Qualification Application should include all items described in Section 1.3. Any notice required under this RFP may be given via telecopy,

provided that the notice is also sent via regular US mail on the same date, and in addition to the telecopy, to the members of WCPS's E/P Team listed above.

Please provide your Qualification Application as soon as possible to the above addresses but no later than ***12:00 NOON Pacific Daylight Savings Time on September 30, 1996.*** This will be your company's only opportunity to validate itself as a Qualified Primary Vendor in accordance with Section 1.3., and you will be notified no later than ***Close of Business October 9, 1996*** as to your status with respect to eligibility to bid on this RFP in accordance with the Qualification criteria. This Qualification Application submission is separate and apart from your response to this RFP. Also, upon establishing your qualification to bid as a Primary Vendor, you will be invited by WCPS to participate fully in WCPS's RFP Competition.

Failure to direct your Qualification Application response to the addresses given above by the closing date contained in this section will result in the ***absolute disqualification*** of your proposal from further consideration under this RFP.

1.4.2. RFP Proposal Submission

The package containing a Qualified Primary Vendor's RFP Proposal Response submission shall be marked "Sealed RFP Proposal" with this RFP title and your organization's name prominently affixed to it.

1.4.2.1. Submission Date

All Qualified Primary Vendor responses to this RFP shall be received NOT LATER THAN 12:00 NOON, PACIFIC STANDARD TIME, November 1, 1996.

1.4.3. Composition of Qualified Primary Vendor's RFP Proposal Response

All Primary Vendor's must submit nine (9) sets (hard copy and diskette copy in IBM DOS format, Microsoft Word 6.0) of two-sided copies of your RFP response. Please send the appropriate number of copies to each to the E/P Team Members, as listed in Section 1.4.1. Please mark one (1) paper copy of your response as "Master Copy." If discrepancies between copies and/or the diskette are found to exist, the "Master Copy" will govern and be relied upon as the "official" response for all submissions. Please send the "Master Copy" of your RFP Response submission to Mr. John Meyer at the address furnished above in Section 1.4.1.

All RFP response proposals shall be typed, double spaced, using 8 1/2" x 11" three-hole punched paper, three-ring bound, with each volume beginning on a new page and

separately tabbed. The RFP response proposals shall contain no colored illustrations nor colored text.

Primary Vendors are requested not to make their proposals elaborate with respect to three-ring binding or presentation. A simple, straightforward, efficient and economically reproduced proposal is strongly recommended. Our proposal E/P procedure places a higher premium on thoroughness and substance of presentation, i.e., responsiveness, than on packaging or quantity of material provided.

1.4.3.1. Content Structure

A Primary Vendor is responsible for any and all costs incurred in the preparation of its response to this RFP. All proposals should consist of the following separate Tabs:

Tab 1 - Executive Summary
Tab 2 - Functional and Technical Requirements
Tab 3 - Cost and Price
Tab 4 - Contract Terms and Conditions

DO NOT INCLUDE COST OR PRICE FIGURES ANYWHERE EXCEPT IN YOUR TAB 3 RESPONSE, THE COST AND PRICE SECTION OF THE RFP PROPOSAL.

All proposals meeting the stated requirements and specifications except for minor exceptions and deviations, shall be considered by WCPS's E/P Team. Failure to meet requirements however, could result in a proposal being disqualified from further consideration in the selection process. However, proposals having minor exceptions and/or deviations shall be considered only if the following conditions are satisfied:

(A) All exceptions and deviations from the specifications are to be explicitly and clearly stated in the Proposal's Executive Summary (Tab 1), and;

(B) All exceptions and deviations are appropriately justified on the basis of performance, delivery schedule and/or relative price, based upon factual considerations.

1.4.3.2. Tab Content

The required content of each Tab of your RFP Proposal Response follows:

Executive Summary (Tab 1)

This section should summarize all key features of your proposal response. All deviations and exceptions from the RFP should be stated, and a brief factual justification must be given. A more detailed justification can be included in the Tab that covers the subject.

Functional and Technical Requirements (Tab 2)

This section should discuss the major aspects of the functional design. You should address;

(1) all areas which result in a potentially high degree of risk,
(2) all areas which impose an unusually high degree of responsiveness,
(3) all areas that are deficient and that could be improved, and;
(4)each section of the RFP and every functional and technical requirement must be addressed in your response. The same article, section or paragraph number and title used in the RFP shall be used for the Primary Vendor's detailed RFP response submission.

Cost and Price (Tab 3)

This section shall include a description of the proposed costs and prices under this RFP for a minimum of a three year and five year term. All pricing information shall be limited solely to this section of your proposal. For purposes of your response you ***must*** provide both a three year and a five year view. (See, Section 10, R10-18 and 19). This section should address all requirements set forth in this RFP as well as any other items pertinent to your pricing proposal such as additional discounts for increased volume, prompt payment, transportation charges (FOB destination), etc. Pricing shall also be firm for all orders placed through December 31, 2001, and shall be based on the engineered, furnished, and installed cost of all applicable goods, software, and services of the most recent vintage and/or technology available in the telecommunications industry. Firm pricing proposals must be guaranteed by each Primary Vendor as being good and available to WCPS for a period of at least one-hundred-eighty (180) days after the initial submission of your RFP.

The provision for the "low-tech" SOA interface as an option for smaller carriers is to be designed and priced as an add-on option. That is, WCPS may choose to include or exclude the interface initially, then add or delete it at a later date, for a

specified cost, without other costs or other operational impacts accruing to the other components of the NPAC/SMS.

Quotes should include, but not be limited to a breakdown in the following items:

1. Unit cost
2. Warranty
3. Maintenance (ongoing support)

Contract Terms and Conditions (Tab 4)

This section shall include any objections to the proposed terms and conditions contained in the Master Contract and Service Agreement, to be provided to qualified vendors. In the event of any such objections, this Tab should provide proposed alternative language for consideration by WCPS.

1.4.4. Clarification, Questions and/or Requests for Additional Information

On **October 18, 1996**, WCPS's RFP E/P Team plans to hold a bidders conference for Qualified Primary Vendors. Prior to the bidders' conference all clarification, questions or requests for information will be submitted in writing no later than October 15, 1996, the closing date for information requests under this RFP. Please send these requests to the members of the E/P Team named in Section 1.4.1.

All questions and responses shall be promptly distributed to all Qualified Primary Vendors under this RFP. Please note that the identity of the requesting company shall be withheld from disclosure. Telephone inquiries will not be accommodated. Requests made by telecopy are expected and appreciated, however, please follow up all telecopied submissions with next day delivery to WCPS's the same E/P Team members mentioned above.

1.4.5. Acceptance Period

All Primary Vendor RFP proposals shall indicate that they are valid for a period of not less than one hundred eighty (180) days from the closing date for submission under this RFP.

1.4.6. Contract Award

WCPS reserves the right;

a) to reject any and all responses,
b) to conduct negotiations with more than one Primary Vendor simultaneously,
c) to add, delete and/or change the terms of this RFP and to issue corrections and/or amendments, or supplements to the RFP, at any time without further notice, for any reason whatsoever,
d) to accept or reject, in whole or in part, any response without giving any reason for its decision,
e) to enter into a contractual arrangement with any Primary Vendor, and it is not obligated or limited to do so because of any event associated with issuance of this RFP,
f) to have any documents submitted by a Primary Vendor reviewed and evaluated by any individuals, including independent consultants, and;
g) to cancel the RFP process for any reason without penalty or liability at any time before a written contract is executed.

1.4.6.1. Factors Relevant to Contract Award

The Contract will be awarded to the responsible Primary Vendor whose offer conforms to this RFP solicitation and which will be most advantageous to WCPS, in WCPS's sole discretion. Therefore, price and other factors will be considered. A final contract award may not necessarily be awarded to the Vendor offering the lowest price.

1.4.6.2. WCPS not Responsible or Obligated Under this RFP

WCPS or any individual member thereof shall not be obligated in any way to make a contractual award as a result of this RFP. In no event shall WCPS or any individual carrier be responsible for the costs of preparing the Primary Vendors' response to this RFP; nor shall WCPS or any individual carrier indemnify or incur any liability whatsoever to Primary Vendors and/or their Sub-Contractors, if any, electing to participate in this RFP process.

No contractual obligations are assumed by WCPS or its members by issuing this RFP, receiving, accepting, and evaluating the Primary Vendors' responses, and/or making a preliminary Primary Vendor selection.

WCPS's RFP E/P Team reserves the right to cancel any agreement if the services or facilities do not pass mutually agreeable acceptance tests. This will be done at no cost or obligation to WCPS's RFP E/P Team, WCPS, or CLNPTF and individual members. The Acceptance Testing Plan will form a part of the Master Contract with the Primary Vendor and will be evaluated after initial database deployment.

WCPS's RFP E/P Team, WCPS, and CLNPTF and individual members reserve the right to negotiate all terms and conditions in order to enter into a formal agreement with the Winning Vendor. This document, the Primary Vendor's response, and full system documentation will form a part of the Master Agreement, if applicable.

No publicity or news releases pertaining to this RFP, responses to this RFP, discussions of any kind regarding the RFP, or the award of any agreement related to the RFP document may be released without the prior express written consent and approval of WCPS's RFP E/P Team and WCPS's members.

All work and materials must comply with all federal and state law, municipal ordinances, regulations, and directions of appropriately appointed members of proper authorities having jurisdiction.

The Primary Vendor, by stating compliance to a requirement in this RFP, agrees that the Primary Vendor has read and understood the requirement and that its compliance is complete and deliverable at no additional cost unless otherwise noted.

This RFP may include unintended errors, omissions, and/or deficiencies. Therefore, the accuracy and completeness of this document and related documents are not guaranteed. In the event that such errors, omissions, and/or deficiencies are discovered by the Primary Vendor, the Primary Vendor shall notify the RFP E/P Team in writing as promptly as possible.

The Primary Vendor is expected to examine the specifications and instructions carefully. Calculation errors shall be the Primary Vendor's risk. In the event of a Primary Vendor's error in price, time or calculations, the quoted terms shall prevail, and the Primary Vendor will bear all risk of loss, without opportunity for recovery from WCPS or its members.

1.5. Evaluation/Procurement of Proposals

Qualified Vendor responses to the RFP will be evaluated by each E/P Team member, with the support of staff in an objective and nondiscriminatory manner. A recommendation will be made from the E/P Team to the members of WCPS on the results of the RFP Competition.

During the Evaluation/Procurement process, Primary Vendors will be responsible for providing all information as requested per the applicable instructions from the RFP and/or

WCPS's E/P Team. Primary Vendors must provide sufficient data to enable the E/P Team to completely and fairly evaluate the proposals based upon the above criteria. ANY DEVIATIONS OR EXCEPTIONS TO THE RFP SHOULD BE NOTED IMMEDIATELY BY THE PRIMARY VENDOR AND CONVEYED TO THE EVALUATION/ PROCUREMENT TEAM. ANY PRIMARY VENDOR WHO DOES NOT COMPLETELY REPLY TO THE RFP DOCUMENT OR SPECIFIC REQUESTS FROM THE E/P TEAM AS REQUESTED, MAY BE ELIMINATED FROM THE RFP COMPETITION AT THE DISCRETION OF THE E/P TEAM.

In the event a Primary Vendor's response is "will not be complied with," or "not agreed to," it shall also indicate the reasons for such disagreement and/or non-compliance and provide an example of alternative language with which it would be willing to comply with or agree to. FAILURE TO PROVIDE AN ACCEPTABLE ALTERNATIVE COULD BE GROUNDS FOR ELIMINATION FROM FURTHER CONSIDERATION UNDER THIS RFP, AT THE DISCRETION OF THE E/P TEAM. All responses must be explained in sufficient detail to convey how compliance will be achieved with the terms of this RFP.

The Primary Vendor that executes the Master Agreement and agrees to the terms and conditions of the Service Agreement with WCPS's E/P Team, will await approval of its signed Master Agreement WCPS's members. WCPS will award the business contemplated by this RFP to the winning vendor.

Section 2: Business Process Flows

The following process flows indicate how the NPAC and NPAC/SMS are used in the various business processes associated with number portability. This information is intended to provide an overview of the role of the SMS in number portability. Details of steps in the processes that do not involve the NPAC or NPAC/SMS, such as interactions between service providers, will be determined by the service providers and are beyond the scope of this document. Specific requirements generated by the process flows are included in the appropriate sections later in the document.

Every effort has been made to ensure verbal descriptions of processes and the attached process flow diagrams match. In the event of a perceived discrepancy, please request clarification but otherwise the process flow will prevail.

2.1 Provision Service Process

This process flow defines the provisioning flow in which a customer ports a telephone number to a new service provider.

The new service provider will obtain authorization to port the customer and notify the old service provider according to processes internal to the service providers. Both the old and new service providers will send a notification to the NPAC/SMS from their SOA systems. When the NPAC/SMS receives the notification(s), it will perform certain validation checks, including that both the old and new service provider has sent a notification. If errors are found or one of the service providers did not send a notification, the SMS will enter into a coordination process described in the next paragraph. Assuming the notifications are valid, the two service providers will complete any physical changes required. At the time new service provider is ready to provide service, it will send an activation notice to the NPAC/SMS. The NPAC/SMS will place an activation time stamp on the update and immediately broadcast the update to all local service providers' ~~networks.~~local SMSs. Upon receiving the update from the NPAC/SMS, all service providers will update their networks. The NPAC/SMS will record any transmission failures and take the appropriate action.

In the case where either the old or new service providers did not send a notification to the NPAC/SMS, the NPAC/SMS will notify the service provider from which it did not receive a notification that it is expecting a notification. If it then receives the missing notification and the notifications indicate agreement between the service providers, the process proceeds as normal. If it still does not receive a notification and if it is the old service provider that failed to respond, the NPAC/SMS will log the failure to respond and then the conflict resolution procedures are implemented. If it was the new service provider that failed to respond, the NPAC will log the failure to respond, cancel the

notification, and notify the old service provider of the cancellation. If there is disagreement among the service providers as to who will be providing service for the telephone number, the conflict resolution procedures will be implemented. Processes for obtaining authorization from the customer to port a number are defined by the service providers. The NPAC is not involved in obtaining or verifying authorization.

From the time the new service provider sends a notification to the time it sends the activation notice, the new service provider may send a message to the NPAC/SMS to cancel the notification. If this occurs, the NPAC/SMS will remove the notification from its database and notify the old service provider that the notification has been canceled.

Also during this time frame, the old service provider may remove their authorization. If this occurs, the NPAC/SMS will place the order in conflict.

(refer to Figure 1 Parts 1 and 2 in Process Flows, Section 17)

2.2 Disconnect Process

When a ported number is being disconnected, the customer and service provider will agree on a date. After an aging period, if any, the service provider will send an update indicating the disconnect to the NPAC/SMS. The NPAC/SMS will broadcast the update to all service providers and remove the telephone number from its database of ported numbers. Upon receiving the update, all service providers will remove the telephone number from their LNP databases. The NPAC/SMS will also send a notification to the service provider recovering the disconnected number to indicate the actual customer disconnect date.

The NPAC/SMS will log the update in history. Calls to the telephone number will be routed as a non-ported number.

In both the service provisioning process and disconnect process, when the NPAC/SMS is performing validity checks (such as confirming that required data fields are filled in), if an error is found, the NPAC/SMS will notify the service provider's with an appropriate error message. The service provider will have to resend the notification to have it processed.

(refer to Figure 3 in Process Flows, Section 17)

2.3 Cancellation Process

A customer may call either the old or the new service provider to cancel the service order. If the customer contacted the old service provider, it needs to first obtain the authorization of the customer before notifying the new service provider. If customer contacted the new service provider, it proceeds to notify the old service provider of the cancellation. The inter-provider notification proceeds according to processes internal to the service providers.

If errors are found or one of the service providers did not send a cancellation notification, the SMS will enter into a coordination process described in the next paragraph. Assuming the notifications are valid, the NPAC/SMS will log the information and cancel the transactions.

In the case where either the old or new service providers did not send a cancellation notification to the NPAC/SMS, the NPAC/SMS will notify the service provider from which it did not receive a notification that it is expecting a cancellation notification. If it then receives the missing notification and the notifications indicate agreement between the service providers, the process proceeds as normal, resulting in the NPAC/SMS canceling the transactions. If it still does not receive a cancellation notification from the missing provider, or the information is incorrect/negative, the conflict resolution procedures are invoked.

(refer to Figure 2 in Process Flows, Section 17)

2.4 Conflict Resolution Process

If service providers disagree on who will serve a particular line number, the NPAC will place the request in "conflict" and notify both service providers that conflict resolution is needed. The new service provider will initiate and coordinate the resolution process by management level escalation.

When a resolution is reached, the NPAC will be notified and will remove the request from "conflict" ~~or cancel it.~~ , cancel it (initiated either by a direct cancellation process or after a time out period of thirty days has expired). The NPAC notification can be sent to the NPAC/SMS either manually or over the SOA interface.

If the NPAC was notified by one of the service providers to remove the request out of conflict, the NPAC in turn will notify both service providers of the “Conflict Off” state. Both service providers need to agree on the removal of the conflict, in particular authorization is sought from the service provider which did not initiate the conflict removal. Once a positive authorization is obtained, the provisioning process proceeds as normal. If authorization was not received, or the authorization was not in agreement, the NPAC notifies both service providers and the request reverts back to the conflict resolution process.

(refer to Figure 4 Parts 1 and 2 in Process Flows, Section 17)

2.5 Disaster Recovery and Backup Process

This Section describes a proposed process flow, please refer to Section 10, requirement R10-13, for the detailed description of the requirement. If there is planned downtime for the NPAC/SMS, the NPAC/SMS will send an electronic notification to the service provider's SOAs that includes information on when the downtime will start, how long it

will be and if they will be required to switch to a temporary "backup" process. Primary Vendor's are required to clearly articulate in their response their specific solutions for managing any downtime experienced by the NPAC/SMS. Downtime is considered planned when the NPAC can provide notification to the service providers at least 2 weeks in advance. If the downtime will be less than 10 minutes, the service providers will remain connected to the primary process and not send any updates during the downtime. If the downtime will be longer than 10 minutes, the NPAC service providers will switch to its proposed "backup" or disaster recovery process as indicated in the notification. There will be a quiet period (minutes) when no updates can be sent in order to allow the NPAC to connect the service providers to the proper process. At the end of the quiet period, processes will proceed as normal. When the primary process is brought back up, the "backup" or disaster recovery process will send an electronic notification to the service provider's SOAs indicating the time when the NPAC will switch them back to the primary process. At the end of the quiet period, processes will continue as normal and the NPAC will synch up the database in its primary SMS with any updates sent to the "backup" or disaster recovery process during the downtime.

If there is unplanned downtime, the NPAC will assess how long the primary process will be down. The NPAC will notify all of the service providers immediately by telephone to the service provider's contact numbers providing the status of the situation and its planned action. If the downtime is expected to be less than 10 minutes, the service providers will remain connected to the primary process and not send any updates during the downtime. If the downtime will be longer than 10 minutes, the service providers will switch to the proposed "backup" or disaster recovery process and later back to the primary using the same process as described for planned downtime. In addition, once the service providers have been switched off the primary process, each service provider will check to see if any updates of newly ported numbers sent to the primary database during the time it went down were not broadcast out. If a service provider finds such updates, the service provider may use internal inter-carrier processes to update its own SCPs and have other carriers update their SCPs with the information in order to ensure service to the affected customers. This will not be needed for disconnect orders. Even if it finds such updates, a service provider may choose to wait until it can begin sending updates to the proposed "backup" or disaster recovery process and then just resend the updates that had failed in the primary database. If a service provider does use internal processes to request updates to SCPs while waiting to be able to send them to the backup or disaster recovery process, the service provider will still resend the updates when the proposed "backup" or disaster recovery process can begin processing them in order to ensure every service provider and the NPAC/SMS receive the update.

Section 3: NPAC Data Administration

3.1 Overview

The NPAC/SMS manages the ported TN information associated with the service provider portability for the LNP service.

3.1.1 Service Data

The Service Data contains global parameters specific to the LNP service.

Examples of some of these parameters are described below. The description presents a logical representation of the data, not an implementation view.

- Time interval for concurrence from both service providers
- Number of retries for download to Local SMS
- Time interval a subscription version stays in conflict

3.1.2 Service Provider Data

Service Provider Data contains information about service providers participating in the LNP service.

3.1.3 Subscription Data

Subscription Data consists of information about the ported TNs.

The data items that need to be administered by Subscription Data Administration functions are described below. The description presents a logical representation of the data, not an implementation view.

R3-1 The NPAC/SMS shall, at a minimum, receive, store, and broadcast the following information on each ported DN: (Descriptions of these items can be found in ~~the glossary that is attached to this RFP as an appendix~~Section 14.)

Data Item	Receive	Store	Regular Broadcast	Disconnect Broadcast
Telephone Number	X	X	X	X
LRN	X	X	X	
Facilities-Based Pro ~~i~~vider ID	X	X	X	
Disconnect Date	X	X		Sent only to provider recovering spare number
DPC for CLASS	X	X	X	
SSN for CLASS	X	X	X	
DPC for LIDB	X	X	X	
SSN for LIDB	X	X	X	
DPC for ISVM	X	X	X	
SSN for ISVM	X	X	X	
DPC for CNAM	X	X	X	
SSN for CNAM	X	X	X	
End-user location (Future Use)				
Billing ID (Future Use)				

Note 1: If a SSN = 0, it implies that DPC is the gateway.
Note 2: See Section 3.1 of the FRS for a summary of the data elements administered and utilized by the NPAC/SMS.

R3-2 The NPAC/SMS shall permit the size of each field identified above to vary. The NPAC may require additional fields for its uses. Additionally, future considerations may require additional types of data to be received, stored, and broadcast by the NPAC/SMS (See Section 13).

3.2 Receiving Data

R3-3 The NPAC/SMS shall be designed to interface electronically with three types of "users". First, large local exchange telecommunications providers will probably interface for purposes of uploading data into the NPAC/SMS and receiving broadcasts from the NPAC/SMS. Second, a small rural telecommunications provider may wish to interface with the NPAC/SMS for purposes of uploading data, but may elect to contract with another provider to maintain its routing information. Such a company, therefore, may not interface with the NPAC/SMS for receiving broadcasts. Third, an interexchange provider may only interface with the NPAC/SMS for purposes of maintaining routing information and, therefore, may not interface with the NPAC/SMS to upload information. Throughout this RFP, the term "user" is used generically. The Service Provider and Service Provider network data scenarios shall be implemented as defined in Sections 6.3 and 6.4 of the IIS.

R3-4 The NPAC shall receive and record data needed to identify, contact, and bill new NPAC/SMS users. For example, the NPAC shall receive the LRNs, portable NXXs, network addresses for interfaces, and billing information. If the new user is a facilities-based service provider, the NPAC/SMS shall verify that the correct facilities-based service provider ID is associated with the new user.

Section 4: Service Provider and Network Data Administration

4.1 Service Provider Data Administration

The data items that need to be administered by Service Provider Data Administration include (but are not limited to):

A. Service Provider Name

B. Facility-based Service Provider Identification

C. Service Provider Address

D. Service Provider Phone

E. Service Provider Contact

F. Service Provider Repair Center Information

G. Service Provider System Data Link Information

R4-1 The NPAC/SMS shall administer the service provider data defined in Section ~~XXX~~3.1.2 of the FRS.

R4-2 The Service Provider scenarios shall be implemented as defined in Section 6.3 of the IIS.

4.2 Service Provider Network Data Administration

Service provider network data contains the NPA-NXXs assigned to the service provider and LRN lists.

R4-3 The NPAC/SMS shall administer the service provider network data defined in Section ~~XXX~~3.1.3 of the FRS.

R4-4 The service provider network data scenarios shall be implemented as defined in Section 6.4 of the IIS.

Section 5: Subscription Administration

Subscription Administration functions allow users to specify data needed for ported numbers. The subscription data indicates how local number portability should operate to meet subscribers' needs. These functions will be accessible to authorized service providers via an interface (e.g., the SOA interface) from their operations systems to the NPAC/SMS and will also be accessible to (and performed by) NPAC personnel.

5.1 Provision

R5-1 The subscription version data associated with each ported DN shall be defined in Section 3.1.3 of the FRS.

R5-2 When a customer wishes to change service providers and keep the same telephone number, the new service provider shall instruct the NPAC/SMS to create a subscription associated with that customer's telephone number. The subscription shall be created in the pending state. The subscription version flow scenarios shall be implemented as defined in Section 6.5.1 of the IIS.

R5-3 When a subscription is in the pending state, the NPAC/SMS shall:

(a) verify the data;

(b) alert the old service provider of the creation of the subscription and allow the old service provider the opportunity to either confirm the data in the subscription or place the subscription into conflict;

(c) allow the new service provider the opportunity to cancel the subscription; and

(d) allow the new service provider the opportunity to activate the subscription when the new service provider effectuates the physical act of changing the customer's service.

The subscription version flow scenarios shall be implemented as defined in Section 6.5.1 of the IIS.

R5-4 It is possible that the old service provider shall send a confirmation prior to the new service provider sending a request to create a subscription. If this occurs, the NPAC/SMS shall:

(a) verify the data;

(b) alert the new service provider of the confirmation;

(c) if the new service provider sends a request to create a subscription within 90 days (tunable parameter), follow the process outlined in R5-3 (except step b); and

(d) if the new service provider does not send a request to create a subscription within 90 days (tunable parameter), delete the confirmation and issue error message.

The subscription version flow scenarios shall be implemented as defined in Section 6.5.1 of the IIS.

R5-5 When a customer who has already ported at least once changes service providers again, a subscription will be created in the pending state and, eventually, in the active state. At that time, the obsolete version of the subscription existing in the active state shall be stored by the NPAC/SMS in the archived state. Each archived version of a subscription shall be stored by the NPAC/SMS for 18 months (tunable parameter). The subscription version flow scenarios shall be implemented as defined in Section 6.5.1 of the IIS.

5.2 Conflict

R5-6 A subscription shall be placed into conflict if: (a) the information provided by the new service provider does not match the information provided by the old service provider or (b) if the NPAC/SMS receives a request to create a subscription for a DN currently in pending. In the second case, both subscription requests shall be placed into conflict. The subscription version conflict scenarios shall be implemented as defined in Section 6.5.5 of the IIS.

R5-7 If a subscription has been placed into conflict the NPAC/SMS shall notify all affected users and save the information associated with the subscription for 30 days. The subscription version conflict scenarios shall be implemented as defined in Section 6.5.5 of the IIS.

R5-8 A subscription which has been placed into conflict shall not be broadcast by the NPAC/SMS until and unless the service providers reach agreement over the appropriate information in the subscription and resubmit an appropriate modification or new request and confirmation.

5.3 Modification

R5-9 The NPAC/SMS shall permit the new service provider to modify a subscription in the pending state. The NPAC/SMS shall verify all modified data. The subscription

version modification scenarios shall be implemented as defined in Section 6.5.2 of the IIS.

R5-10 The NPAC/SMS shall permit the service provider to modify a subscription in the active state. The NPAC/SMS shall verify all modified data and rebroadcast the subscription. The subscription version modification scenarios shall be implemented as defined in Section 6.5.2 of the IIS.

5.4 Validations

R5-11 When the NPAC/SMS receives and broadcasts data it shall perform the following validations: (a) all data must be in the proper format and (b) if a DN is being ported, (1) the NPA-NXX and the LRN must be associated with a valid facilities-based provider, (2) the new facilities-based ID must match the new LRN, and (3) the NXX must be portable,

R5-12 If a confirmation is sent by the old facilities-based provider, the NPAC/SMS shall verify that the information sent by the old facilities-based provider matches the information sent by the new facilities-based provider.

5.5 Error/Success Messages

R5-13 Whenever the NPAC/SMS is asked to perform a task or verify data, the NPAC/SMS shall issue an error message to the appropriate company(ies) if the task can not be successfully completed or if the data is improper. The error message shall, when possible, identify the cause of the failure or the improper data.

R5-14 Whenever the NPAC/SMS completes a task it was asked to perform or verifies that data is proper, the NPAC/SMS shall issue a success message to the appropriate company(ies).

5.6 Broadcasting Data

R5-15 When a subscription has been activated or modified in the active state, the NPAC/SMS shall broadcast the subscription to all users. If the NPAC/SMS is unable to transmit the data to a particular user, the NPAC/SMS shall repeat the

attempt twice (tunable parameter) and, if the data has still not been successfully transmitted, contact the user and rebroadcast the data once the problem is solved. Once a subscription has been broadcast to at least one user, the subscription shall be in the active state. The subscription version broadcast scenarios shall be defined in Sections 6.5.1.5 through 6.5.1.7 of the IIS.

R5-16 When the NPAC/SMS receives notification that a customer has disconnected, the NPAC/SMS shall broadcast a disconnect message and remove the DN from the database of ported numbers. The subscription version disconnect scenarios shall be implemented as defined in Section 6.5.4 of the IIS.

5.7 NPA Splits and Mass Updates

R5-17 The NPAC/SMS will accept either the old or the new NPA from a SOA during the permissive dialing period, even for the same service order.

R5-18 The SOA and local SMS will accept either the new or old NPA in the NPAC/SMS responses during the permissive dialing period.

R5-19 The NPAC/SMS shall send only the new NPA upon a download, during the permissive dialing period.

R5-20 For ported TNs not ported during the permissive dialing period, the local SMS will locally perform any required mass updates.

R5-21 Any LRN changes caused by the NPA split will be independently performed as mass updates by the NPAC. The service provider associated with the LRN initiates the request with the NPAC to perform the mass change.

R5-22 The NPA split scenarios shall be implemented as defined in Section 6.6.1 of the IIS.

R5-23 The mass update of local SMS subscription data shall be implemented as defined in Section 6.6.4 of the IIS.

5.8 Miscellaneous

R5-2~~2~~4 The NPAC/SMS may receive requests from a local SMS to start a network data download (by specifying a specific start time) after a planned or unplanned outage. The NPAC/SMS will respond by downloading the requested data until resynchronization is established. The control of events to initialize/resynchronize the local SMS shall be implemented as defined in Section 6.6.1 of the IIS.

R5-2~~3~~5 The NPAC/SMS shall notify all SOAs and service providers' local SMSs of a scheduled downtime of the NPAC/SMS. This will be done in some tunable amount of time before the scheduled outage. This notification shall be implemented as defined in Section 6.6.2 of the IIS.

R5-26 The NPAC/SMS shall filter, at an NPA-NXX level, the broadcasts and other messages sent to the service provider's local SMS.

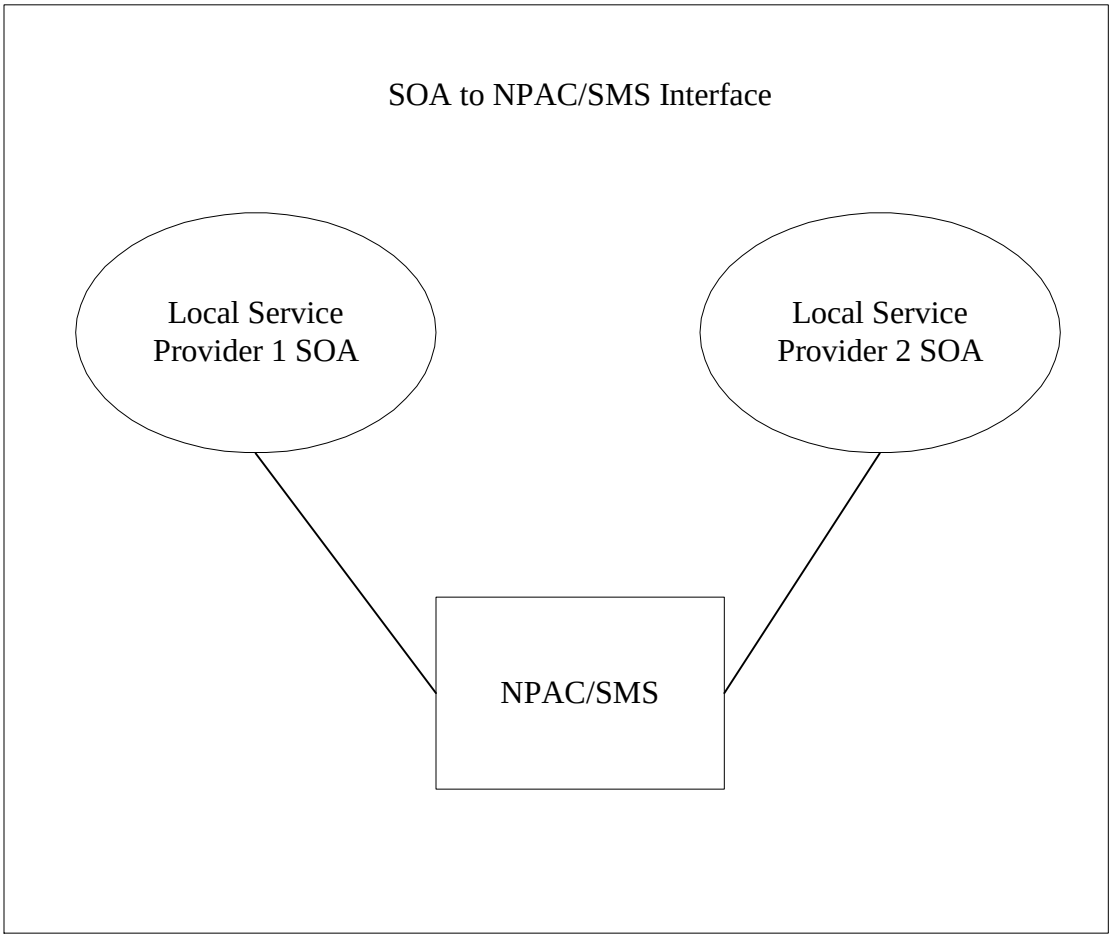
R5-27 The NPAC/SMS shall allow the service provider to specify the NPA-NXXs for which it wishes to receive information.

Section 6: NPAC/SMS Interfaces

Two interfaces to the NPAC/SMS shall be supported. The first interface shall be between the NPAC/SMS and the service provider's Service Order Activation platform and the second shall be between the NPAC/SMS and the Local SMSs. Both of the interfaces shall support two-way communications.

6.1 SOA to NPAC/SMS Interface

The SOA to NPAC/SMS Interface could be used by a variety of local service provider systems for retrieving and updating subscription data in an NPAC/SMS. The types of systems that are expected to use this interface are Service Provisioning OSs and/or Gateway Systems.



6.1.1. Request Administration

The SOA to NPAC/SMS Interface will support four types of transactions: subscription request and audit request transactions from the front end system (e.g., the SOA) interface users, and response and notification transactions from the NPAC/SMS. The Interface will require security features to ensure that data is not corrupted by unauthorized access. Security management is outside the scope of the interface, however, the Interface user will be required to provide parameters to support security management at the NPAC/SMS.

R6-1 Associations on these application to application interfaces must use strong authentication.

R6-2 Each subscription administration request sent over the Interface shall be capable of supporting multiple independent transactions. One failed item in a request will not cause other items in the request to fail. See ANSI standard T1.246, *Operations, Administration, Maintenance and Provisioning (OAM&P) - Information Model and Services for Interfaces between Operations Systems across Jurisdictional Boundaries to Support Configuration Management - Customer Account Record Exchange (CARE)* for an example of a GDMO (ISO 10165-4) description of an interface that can deal with bunched transactions.

R6-3 Each subscription administration request shall be acknowledged with at least one response transaction from the NPAC/SMS. Some requests may be acknowledged more than once. For example, after validation processing is completed a response transaction would be sent back to the user with either a positive acknowledgment or a negative acknowledgment with an error message indicating the results of the validation.

6.1.2 Subscription Administration

Subscription Administration provides functionality in creating or modifying subscriptions and activating or deleting them from the networks. Based on security parameters, users of the interface shall be able to do the following:

R6-4 Add new versions of subscription data, as well as cancel or modify a specific version of subscription data.

R6-5 Retrieve subscription data, including either specific versions of a subscription or all versions.

R6-6 Request the activation or deletion of subscription data.

6.1.3 Audit Processing

R6-7 The NPAC/SMS shall support maintenance audits which occur on a periodic basis. See R8-4 through R8-6.

6.1.4 Notifications

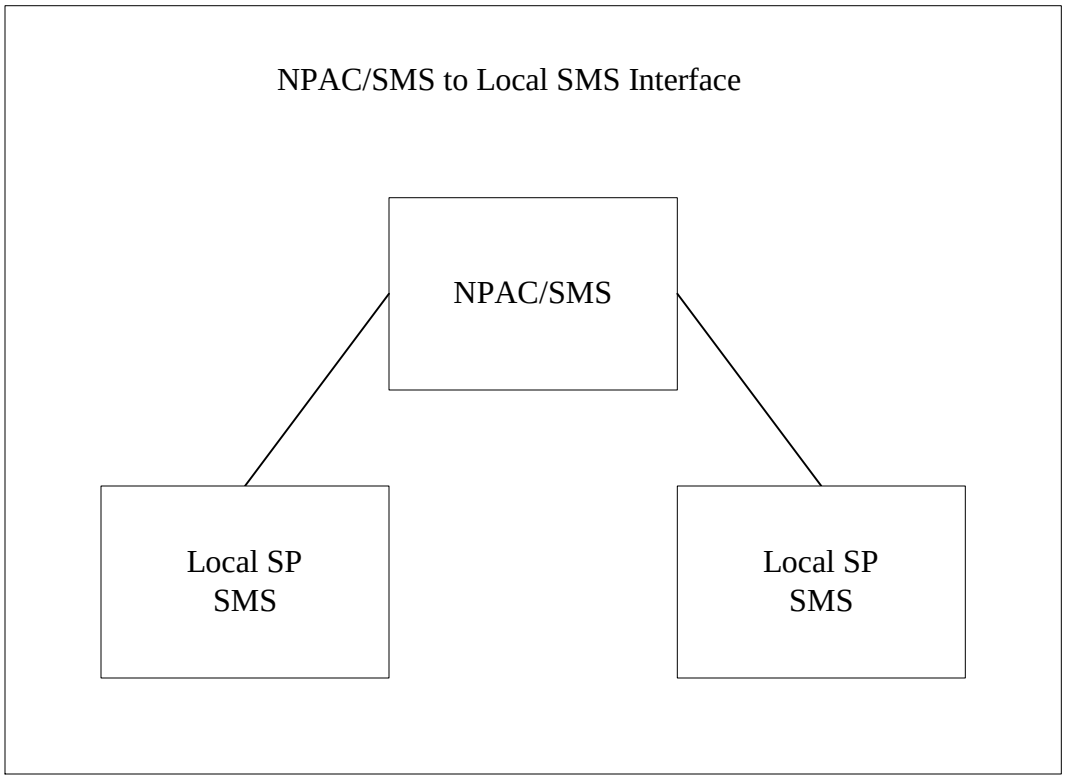
NPAC/SMS shall have functionality to send notifications to service providers based on parameters which are tunable by the NPAC/SMS Administrator. NPAC/SMS shall be able to do the following via the interface:

R6-8 Notify a new or an old service provider that they haven't provided authorization for a transfer of service for a TN.

R6-9 Notify an old service provider that the Due Date for a subscription has been modified.

6.2 NPAC/SMS to Local SMS Interface

The NPAC/SMS to Local SMS Interface could be used to send subscription data and audit requests to a variety of service provider systems. The types of systems that is expected to use this interface are Local SMSs (or SMS-like functionality at LNP SCPs) and/or Gateway Systems. The interface will require security features to ensure that data is not corrupted by unauthorized access Security management is covered in Section 7, however, the interface user will be required to provide parameters to support security management at the NPAC/SMS.



6.2.1 Transaction Administration

The NPAC/SMS to Local SMS Interface will support five types of transactions: subscription download transactions from the NPAC/SMS, audit requests from the NPAC/SMS, network data download transactions from the NPAC/SMS, response transactions from the Local SMS, and requests from the Local SMS that specific transactions be resent.

R6-10 Interface users shall specify their user-identification, system identification, and password to be able to use the Interface.

R6-11 Each subscription download request sent over the interface shall be capable of supporting multiple independent transactions. One failed item in a request will not cause other items in the request to fail.

R6-12 Each subscription download request shall be acknowledged with at least one response transaction from the Local SMS. A response transaction shall be sent back to the NPAC/SMS with either a positive acknowledgment or a negative acknowledgment which may include a request that the transaction be sent again.

R6-13 Each audit request sent over the interface shall be for a single transaction or for a range of transactions.

R6-14 Each audit request shall be acknowledged with at least one response transaction from the Local SMS. A response transaction shall be sent back to the NPAC/SMS with either a positive acknowledgment for those TNs which passed audit and a negative acknowledgment for those TNs which failed audit as well as only a negative acknowledgment for those TNs which failed audit.

R6-15 A local SMS shall be able to request the NPAC/SMS to resend a subscription based on its TN or a block of subscriptions based on a time window specified in the request. This function might be provided by allowing for an audit request from the local SMS.

R6-16 Each network data download request shall be acknowledged with one response transaction from the Local SMS. A response transaction shall be sent back to the NPAC/SMS with either a positive acknowledgment or a negative acknowledgment which may include a request that the transaction be sent again.

6.2.2 Network Subscription Administration

Network Subscription Administration provides functionality in activating, modifying, or deleting subscription data from the network and in requesting audits. The NPAC/SMS, via its interface to Local SMSs shall be able to do the following:

R6-17 Add new subscription data, as well as delete or modify specific subscription data.

R6-18 Request audits of subscription data, including either a specific subscription or a range of subscriptions.

6.3 Interface Transactions

The CMIP protocol provides for seven types of transactions over the interface (Reference: ISO 9595 and 9596). They are Create, Delete, Set, Get, Cancel-Get, Action, and Event-Report. The first six transactions are originated by the manager, and affect objects contained in the agent. The ~~Notification~~Event-Report transaction is created by the agent and is used to give notice to the manager that something of interest to the manager has happened to an object in the agent system. The object model has been designed in terms of using these transactions in a manager-agent relationship.

6.4. Interface and Protocol Requirements

While it is expected that dedicated links will be used for the interfaces, switched connections should also be supported. Reliability and availability of the links will be essential and high capacity performance will be needed.

R6-19 The SOA to NPAC/SMS Interface and the NPAC/SMS to Local SMS Interface shall be an open, non-proprietary interface.

6.4.1 Protocol Requirements

R6-20 All system to system interfaces shall be implemented as defined in Section 2.2 of the IIS.

R6-21 Multiple associations per service provider may be required.

R6-22 An additional, alternative NPAC/SMS to User-SOA interface shall be provided by the vendor to support communications via dial-up modem using PPP and a vendor defined, secure and simple low-cost message protocol. A non-inclusive list of possible message protocols is shown below:

a) A fixed format record for each SOA function that can be sent to, or received from, the NPAC/SMS

b) Sequential Query Language (SQL)

c) Any other message protocol proposed by the vendor

R6-23 The vendor defined, secure, simple low-cost message protocol, requested in R6-22, shall provide all SOA interface functionality that is required on the NPAC/SMS to User-SOA CMISE interface.

R6-24 An application shall be provided that can operate on Windows 95™ or Windows NT™ that will allow the user to easily enter service order data and interface with the NPAC/SMS via the secure, simple low-cost message protocol.

R6-25 Describe any changes or losses in performance, if any, resulting from the use and implementation of the secure, simple low-cost message protocol described in R6-22.

6.4.2 Interface Performance Requirements

For purposes of measuring the NPAC/SMS performance we used the characteristics listed below:

1. 20% of the telephone numbers (TNs) downloads will be requested by the SOA as a range.
2. Each download range request from the SOA will contain an average of 20 TNs.
3. 80% of TN downloads will be requested by the SOA as a single TN.
4. The goal of the service providers is to have the NPAC/SMS be capable of downloading 25 TNs per second to minimize the time required to port large business customers.

R6-26 Both the SOA to NPAC/SMS and the NPAC/SMS to Local SMS interfaces shall be available on a 24 by 7 basis.

R6-27 A 99.9 % availability rate shall be maintained for both interfaces.

R6-28 The peak rate which shall be supported by each NPAC/SMS interface association shall support the porting 25 TNs per second.

R6-29 The peak rate shall be supported for at least 5 minutes periods.

6.4.3 Interface Specification

The Primary Vendor will be requested to build to an existing interface specification that is being/will be used for other NPAC/SMS's. The interoperable interface model is specified in terms of ISO 10165-4 "Generalized Definition of Managed Objects" (GDMO). A copy of the interoperable interface specification should be available in July 1996 for distribution to Primary Vendors bidding on the California NPAC/SMS.

R6-300 Any additions/modifications to the interface specification will be documented and become the property of WCPS, which may make them public at any time.

R6-311 The NPAC/SMS Interoperable Interface Specification (IIS) shall define the interface between the NPAC/SMS and the SOA.

R6-322 The IIS shall define the interface between the NPAC/SMS and the local SMS.

R6-333 Section 6 of the IIS shall define the message flow scenarios between the NPAC/SMS and SOA systems, and between the NPAC/SMS and local SMSs.

R6-344 Section 7 of the IIS shall define the GDMO object definitions managed and utilized by the NPAC/SMS.

R6-355 Unless otherwise stated in this RFP, the requirements in the IIS shall take precedence over requirements in this RFP.

R6-366 Unless otherwise stated in this RFP, the requirements in the NPAC/SMS Functional Requirements Specification (FRS) shall take precedence over requirements in this RFP.

Section 7: Security Requirements

Introduction

In addition to the general security requirements based on the user interface paradigm in Section 7.1 through 7.7, there are requirements for the security on an OSI application to application interface (such as the one specified in Section 6 for the SMS to SMS and SMS to SOA interfaces). Section 7.8 describes such a security environment.

7.1 Identification

A user identification is a unique, auditable representation of the user's identity within the system. The SMS requires all system users, both individuals and remote machines, to be uniquely identified to support individual accountability.

R7-1 Unique user identification codes (user-ids) must be utilized to identify individuals and remote machines.

R7-2 SMS must require users, i.e., individuals and remote machines, to identify themselves with their assigned user-id before performing any actions.

R7-3 SMS must maintain internally the identity of all currently active users.

R7-4 Every process running on SMS must have associated with it the user-id of the invoking user (or the user-id associated with the invoking process).

R7-5 SMS must disable user-ids after a period of time during which the user-id has not been used. The time must be NPAC-specific with a system delivered default of 60 days.

R7-6 SMS must provide a complementary mechanism or procedure for the re-instatement or deletion of disabled user-ids.

R7-7 SMS must support the temporary disabling of user-ids.

R7-8 The mechanism that disables user-ids should provide an option for automatic reactivation.

R7-9 SMS must control and limit simultaneous active usage of the same user-ids by allowing only one active login. When the second login is entered, the system will ask if the first login can be disconnected. If the user replies yes, the second login can continue; however, if the user replies no, the second login is terminated.

7.2 Authentication

The identity of all system users, both individuals and remote machines, must be verified or authenticated to enter the system, and to access restricted data or transactions.

R7-10 SMS must authenticate the identity of all system users, both individuals and remote machines, prior to their initially gaining access to SMS.

R7-11 SMS must not support ways to bypass the identity authentication mechanisms.

R7-12 SMS must protect all internal storage of authentication data so that it cannot be accessed by any unauthorized user.

7.2.1 Password Requirements

R7-13 SMS shall not provide a mechanism whereby a single password entry can be shared by multiple user-ids.

R7-14 SMS must not prevent a user from choosing a password that is already associated with another user-id.

R7-15 SMS must store passwords in a one-way encrypted form.

R7-16 Encrypted passwords must not be accessible to non-privileged users.

R7-17 Unencrypted passwords must not be accessible to any users, including NPAC personnel.

R7-18 SMS must automatically suppress or fully blot out the clear-text representation of the password on the data entry device, e.g., terminal.

R7-19 Passwords should not be sent over public or shared data networks in clear text.

R7-20 SMS must not allow for any password to be null.

R7-21 SMS must provide a mechanism to allow passwords to be user-changeable. This mechanism must require re-authentication of the user identity.

R7-22 The NPAC must have a mechanism to reset passwords.

R7-23 SMS must enforce password aging, i.e., passwords must be required to be changed after a NPAC-specific time. The system supplied default shall be 90 days.

R7-24 SMS must provide a mechanism to notify users in advance of requiring them to change their passwords. This can be done by one of the following methods:

(1) SMS will notify users a NPAC-specific period of time prior to their password expiring. The system supplied default shall be seven days.

(2) Upon password expiration, SMS will notify the user, but allow an NPAC-specific subsequent number of additional logons prior to requiring a new password. The system supplied default shall be two additional logins.

R7-25 Password must not be reusable by the same individual for an NPAC-specific period of time. The system supplied default shall be six months.

R7-26 SMS must provide a method of ensuring the complexity of user-entered passwords that meets the following requirements:

(1) Passwords must contain a combination of at least six alphanumeric characters including at least one alphabetic and one numeric or punctuation character. If the system does not distinguish between upper and lower case alphabetic characters, the minimum acceptable length is eight characters.

(2) Passwords must not contain the associated user-id.

R7-27 SMS-supplied password generation algorithms must meet the following requirements:

(1) Passwords must be "reasonably" resistant to brute-force password guessing attacks, i.e., the total number of system generated passwords must be on the same order of magnitude as what a user could generate using the rules specified in requirement 7-26 (1) above.

(2) The generated sequence of passwords must have the property of randomness, i.e., consecutive instances must be uncorrelated and the sequences must not display periodicity.

7.3 Access Control

Access to the SMS and other resources must be limited to those users that have been authorized for that specific access right.

7.3.1 System Access

R7-28 SMS must allow access to authorized users and authorized remote systems.

R7-29 SMS must provide a procedure for the initial entry or modification of authorized users and authentication information.

R7-30 SMS must not provide any default user-ids that can permit unauthenticated SMS access.

R7-31 SMS's login procedure should be able to be reliably initiated by the user, i.e., a trusted communications path should exist between SMS and the user during the login procedure.

R7-32 SMS must disconnect or re-authenticate users after an NPAC-specific period of non-use. The system supplied default shall be 60 minutes.

R7-33 The SMS login procedure must exit and end the session if the user authentication procedure is incorrectly performed an NPAC-specific number of times. The system supplied default shall be three times.

R7-34 SMS must provide a mechanism to immediately notify the NPAC when the above threshold is exceeded.

R7-35 When the above threshold has been exceeded, an NPAC-specific interval of time, not to exceed 60 seconds, must elapse before the login process can be restarted on that I/O port.

R7-36 SMS must not suspend the user-id upon exceeding the above threshold.

R7-37 SMS must perform the entire user authentication procedure even if the user-id that was entered was not valid.

R7-38 Error feedback must provide no other information except "invalid," i.e., it must not reveal which part of the authentication information is incorrect.

R7-39 SMS should provide a mechanism to exclude or include users based on time-of-day, day-of-week, calendar date, etc.

R7-40 SMS should provide a mechanism to exclude or include users based on method or location of entry.

R7-41 SMS must provide a mechanism to limit the users authorized to access the system via dial-up facilities.

R7-42 SMS must provide a mechanism to limit system entry for privileged NPAC users on an NPAC-specific network access or per-port basis.

R7-43 Since some form of network access, e.g., dial-in, Wide Area Network, or Internet, is provided by SMS, SMS must provide a strong authentication mechanism. For example, the authentication mechanism could be a private or public key encryption-based mechanism, an additional password, and/or smart card to validate the user or remote system. For remote machines, public key encryption may be required in conjunction with dedicated private lines. For dial-in users (NPAC administrative and NPAC operations), smart cards are required.

R7-44 A mechanism must exist to end the session through secure logoff procedures.

R7-45 SMS must provide an advisory warning message upon system entry regarding unauthorized use, and the possible consequences of failure to meet those requirements.

R7-46 The message must be NPAC-specific to meet their own requirements, and any applicable laws.

R7-47 SMS must be able to display a message of up to 20 lines in length. This message should be displayed at the first point of entry. If possible, the message should

appear before the logon process. As part of the delivered software, the following is an example of the default message that must be included:

NOTICE: This is a private computer system.

Unauthorized access or use may lead to prosecution.

R7-48 Upon successful access to the system, the following must be displayed:

(1) Date and time of the user's last successful system access.

(2) The number of unsuccessful attempts by that user-id to access the system, since the last successful access by that user-id.

R7-49 SMS must allow only the NPAC well-defined privileged users responsible for security administration to authorize or revoke users.

R7-50 Procedures for adding and deleting users must be well defined and described in the NPAC security documentation.

7.3.2 Resource Access

R7-51 Only authorized users shall be able to access the data that is part of or controlled by the SMS system.

R7-52 Each service provider's data must be protected from access by unauthorized users.

R7-53 Only authorized users shall be able to access the transactions, data, and software that constitute the SMS.

R7-54 The executable and loadable software must be access controlled for overwrite and update, as well as execution rights.

R7-55 Control of access to resources must be based on authenticated user identification.

R7-56 Encryption may be used to augment the access control mechanisms, but must not be used as a primary access control mechanism for sensitive data.

R7-57 For every resource controlled by SMS, it must be possible to grant access rights to a single user or a group of users.

R7-58 For every resource controlled by SMS, it must be possible to deny access rights to a single user or a group of users.

R7-59 It will be necessary to restrict user access to information based on the data content of a specific field, attribute, table, record, etc.

R7-60 Modification of the access rights to a resource must only be allowed by the NPAC.

R7-61 SMS must provide a mechanism to remove access rights to all resources for a user or a group of users.

R7-62 The access control mechanism's data files and tables must be protected from unauthorized access.

7.4. Data and System Integrity

R7-63 SMS must be able to identify the originator of any accessible system resources.
R7-64 SMS must be able to identify the originator of any information received across communication channels.

R7-65 SMS must provide mechanisms or procedures that can be used to periodically validate the correct operation of the system. These mechanisms or procedures should address: (1) Monitoring of system resources (2) Detection of error conditions that could propagate through the system (3) Detection of communication errors above/below an NPAC-specific threshold (4) Detection of Link Outages.

R7-66 SMS must be designed and developed to protect data integrity. This should include some or all of the following:

(1) Proper rule checking on data update

(2) Proper handling of duplicate/multiple inputs

(3) Checking of return status

(4) Checking of inputs for reasonable values

(5) Proper serialization of update transactions

R7-67 NPAC documentation must contain recommendations for running database integrity checking utilities on a regular basis.

7.5 Audit

7.5.1 Audit Log Generation

R7-68 SMS must generate an audit log that contains information sufficient for after-the-fact investigation of loss or impropriety and for appropriate response, including pursuit of legal remedies. The audit data shall be available on-line for a minimum of 90 days, and archived off-line for a minimum of two years.

R7-69 The user-identification associated with any SMS request or activity must be maintained, so that the initiating user can be traceable.

R7-70 SMS must protect the audit log from unauthorized access.

R7-71 Only well-defined privileged NPAC personnel can modify or delete any or all of the audit log.

R7-72 The audit control mechanisms must be protected from unauthorized access.

R7-73 SMS must cause a record to be written to the security audit log for at least each of the following events:

(1) Invalid user authentication attempts

(2) Logins and activities of NPAC users

(3) Unauthorized data or transaction access attempts

R7-74 Auditing of NPAC actions must not be able to be disabled.

R7-75 For each recorded event, the audit record must contain, at a minimum:

(1) Date and time of the event

(2) User identification including associated terminal, port, network address, or communication device

(3) Type of event

(4) Name of resources accessed

(5) Success or failure of the event

R7-76 Actual or attempted passwords must not be recorded in audit logs until after an NPAC-specific threshold of consecutive login failures. The SMS supplied default shall be three failures.

7.5.2 Reporting and Intrusion Detection

R7-77 SMS must provide post-collection audit analysis tools that can produce exception reports, summary reports, and detailed reports on specific data items, users, or communication failures.

R7-78 The NPAC must be able to independently and selectively review the actions of any one or more users, including other NPAC users, based on individual user identity.

R7-79 SMS must provide tools for the NPAC to monitor the activities of a specific network address or terminal in real time.

R7-80 SMS should contain a real-time mechanism that is able to monitor the occurrence or accumulation of security auditable events that may indicate an imminent security violation. This mechanism shall be able to notify the NPAC immediately when thresholds are exceeded, and if the occurrence or accumulation of these security relevant events continues, SMS shall take the least disruptive action to terminate the event.

7.6 Continuity of Service

R7-81 No service provider action, either deliberate or accidental, should cause the system to be unavailable to other users.

R7-82 SMS should detect and report conditions that would degrade service below a pre-specified minimum.

R7-83 Procedures or mechanisms must be provided to allow recovery after a system failure or other discontinuity without a protection compromise.

R7-84 Procedures shall be documented for software and data backup and restoration.

R7-85 The system must contain a database containing the exact revision number of the latest software installed.

7.7 Software Vendor

R7-86 The SMS software vendor must have a corporate policy governing its internal development of software. This policy must contain specific guidelines and requirements that are aimed at the security of its products, and are applicable throughout the software life cycle.

R7-87 The SMS software vendor shall not design any mode of entry into the SMS for maintenance, support, or operations that would violate or bypass any security procedures.

R7-88 The SMS software vendor shall not design any mode of entry into the SMS for maintenance, support, or operations that is not a documented feature of the SMS.

7.8 OSI Security Environment

This section examines potential threats to the NPAC/SMS interfaces and proposes a set of security requirements to thwart such threats.

The security mechanisms described in the OSI Security segment are meant to illustrate the level of security and flexibility that is required for the OSI interfaces specified. The response to the RFP may propose different security mechanisms than the ones described. However, such security mechanisms should provide at least the same level of security and at least the same level of flexibility as the mechanisms described. The proposed mechanisms shall not be more difficult to manage, and should not require more processing or transmission capacity than the mechanisms described below.

7.8.1 Threats

Attacks against the NPAC/SMS may be perpetrated in order to achieve any of the following:

Denial of service to a customer by placing wrong translation information in the SMS

Denial of service to a customer by preventing a valid message from reaching the SMS

Disrupting a carrier's operations by having numerous spurious calls (to users who are not clients of that carrier) directed to that carrier

Switching customers to various carriers without their consent

Disrupting the functioning of the NPAC/SMS by swamping it with spurious messages.

7.8.2 Security Services

The threats enumerated above can be thwarted by using the following security services:

R7-89 Authentication (at association setup)

R7-90 Data origin authentication for each incoming message

R7-91 Integrity - detection of replay, deletion or modification to a message

R7-92 Non-repudiation of origin

R7-93 Access control - allowing only authorized parties (i.e., carriers serving a given customer) to cause changes in the NPAC/SMS database.

7.8.3 Security Mechanisms

This section outlines the requirements for specific security mechanisms to support the security services enumerated above. For simplicity of presentation and without loss of generality, it assumes that information in the NPAC/SMS is modified only in response to CMIP notifications from authorized entities.

7.8.3.1 Encryption

R7-94 Since non-repudiation must be supported, a Public Key Crypto System (PKCS) must be used to provide digital signatures. Since there is no requirement for confidentiality service there is no need for any additional encryption algorithms. The NPAC/SMS shall support one of the digital signature algorithms listed in the OIW Stable Implementation Agreement, Part 12, 1995.

R7-95 If a digital signature based on RSA encryption is chosen then the size of the modules of each key shall be at least 600 bits. If another algorithm is chosen then the size of the key(s) shall be chosen to provide a level of security commensurate with RSA encryption with a 600-bits modules.

R7-96 The digital signature algorithm shall be applied to ASCII representation of the signed data fields, without any separators between those fields or any other additional characters.

7.8.3.2 Authentication

R7-97 Strong, two-way peer authentication at association setup time shall be provided by using an authenticator (based on the authenticator used for the Trouble Administration application of Electronic Bonding as described in Committee T1 Technical Report No. 40 "Security Requirements for Electronic Bonding Between Two TMNs") consisting of:

- The unique identity of the sender
- The Generalized Time corresponding to the issuance of the message, each party is responsible to assure that its system clock is accurate to within two minutes of GMT
- A sequence number (equal to zero for association request and association response messages)
- A key identifier
- Any additional parameters required by the chosen digital signature algorithm, as specified in OIW Stable Implementation Agreement, Part 12, 1995
- The digital signature of the sender's identity, Generalized Time and sequence number listed above.

R7-98 The authenticator shall be conveyed in the CMIP access control field. (An appropriate syntax for this EXTERNAL field shall be provided.)

7.8.3.3 Data Origin Authentication

R7-99 Every subsequent CMIP message that contains the access control field shall carry the authenticator described above in that field. Each party maintains a separate counter for the sequence number it uses. Every time the authenticator is used the value of the sequence number shall be incremented by one.

7.8.3.4 Integrity and Non-repudiation

R7-100 Because CMIP notifications do not have an access control field, all the notifications defined for the number portability application shall contain a security field. The syntax of the security field shall correspond to the authenticator defined above.

R7-101 The values of the components of the authenticator shall also be as specified for the authenticator above, except that the digital signature

shall apply to all the fields in the notification, except the security field, in the order in which they appear, followed by the Generalized Time and the sequence number. This ensures data origin authentication, integrity and non-repudiation of origin for each notification. In particular, the Generalized Time and the sequence number allow detection of deletion, replay and delay.

R7-102 All the notifications shall be sent in the confirmed mode.

7.8.3.5 Access Control

R7-103 The NPAC/SMS shall be responsible for access control. In particular, it will assure that only authorized parties (current and future service providers for a given customer) can change information related to the number associated with that customer.

R7-104 The only initiator-provided access control information that shall be used to this effect is the authenticated identity of the sender of the message that would result in a modification to the NPAC/SMS database, and the value of the Generalized Time in that message (it should be within five minutes of the NPAC/SMS system clock).

7.8.3.6 Audit Trail

R7-105 The NPAC/SMS shall keep a log (as defined in ISO/IEC 10164 parts 6 and 8, 1992) of all incoming messages that result in the setup or termination of associations, all invalid messages (invalid signature, sequence number out of order, Generalized Time out of scope, sender not authorized for the implied request) as well as all incoming messages that may cause changes to the NPAC/SMS database.

7.8.3.7 Key Exchange

R7-106 There shall be an exchange of keys between the NPAC and each carrier it serves. During this exchange each party shall provide the other with a list of keys. The list shall be provided in electronic form. The originator of list of keys shall also provide the receiver with signed (in ink) paper copy of the MD5 hashes of the keys in the list. The lists can be exchanged in person or remotely. If the lists are exchanged remotely, they shall be conveyed via at least two different channels (e.g., a diskette sent via certified mail and file sent via e-mail).

R7-107 Upon remote reception of a list of keys the recipient shall send an acknowledgment to the sender of the list. The acknowledgment shall consist of the MD5 hash of each one of the keys in the list. The

acknowledgment shall be provided in electronic form via at least two different channels. In addition, the recipient shall call the sender by phone for further confirmation, and provide the sender with the MD5 hash of the whole list.

R7-108 The NPAC shall issue periodically (e.g., once a month) a paper list of the MD5 hashes of all the public keys it uses and those of its clients. The list shall be sent to each client. Upon reception of the list and verification of its own the NPAC's public keys hashes, the client shall return an acknowledgment (by phone or mail) to the NPAC.

R7-109 Each list shall consist of 1000 encryption keys, numbered from 1 to 1000, and 10 Key Encryption Keys (KEK), numbered from 1001 to 1010. Only encryption keys shall be used for digital signatures for normal number portability operations. They shall range in size (if RSA encryption is used) from 600 bits to 900 bits. (Larger keys shall be used in future years.) KEKs shall be used only to transmit a new list of keys, if necessary. The whole new list will be signed using a KEK. KEK sizes shall range from 1000 bits to 1200 bits (if RSA encryption is used). Keys in subsequent list shall be numbered from 2000 to 3010, 3000 to 4010, etc.

R7-110 A new encryption key can be chosen with every message that contains a key identifier. After the usage of a key has stopped, that key shall not be used again. The key shall be changed every time there is a suspicion that the key has been compromised. The key shall be changed at least once a year. The keys used during a year shall be larger than the keys used the previous year by at least 20 bits.

Section 8: Audit Administration

Overview

The NPAC/SMS will provide three types of functionality to insure database integrity between service providers' SOA/SMS and the NPAC/SMS. The service provider can verify what is in the NPAC/SMS, the NPAC/SMS can verify what is in a local SMS, and the NPAC/SMS can initiate periodic audits against local SMSs.

8.1 Service Provider Verify of Data in NPAC/SMS

R8-1 A local SMS or SOA will be able to request data from the NPAC/SMS for a given TN or a range of TNs. The local SMS or SOA may request all data for a TN or specific fields.

R8-2 For audit requests from a local SMS or SOA to the NPAC/SMS, the size of the range of TNs will be limited by a tunable parameter.

R8-3 Only the old and new service providers can request data for records in a pending or conflict state.

8.2 Periodic Maintenance Audits

~~R8-4 The NPAC/SMS will perform bulk periodic maintenance audits against local SMS's data. The request may specify individual or ranges of TNs and specific data fields to be returned or that the local SMS return all data associated with the TNs. This type of audit will be performed via FTP as opposed to over the CMISE interface.~~

~~R8-5 NPAC personnel will be able to specify that an audit be initiated either immediately or at a future time.~~

~~R8-6 NPAC personnel will be able to monitor the status of periodic audits~~

The NPAC/SMS will support periodic maintenance audits of subscription data. These audits, including the comparison of local SMS data to the NPAC/SMS data, and the initiation of any resulting corrective action, will be performed by the local SMS.

R8-4 The NPAC/SMS shall maintain a secure site that will allow service providers to retrieve copies of the NPAC/SMS's subscription data via the File Transfer Protocol (FTP).

R8-5 The NPAC/SMS shall periodically place time stamped copies of its subscription data on the secure site described in R8-4. These copies of the subscription data

shall be in files, with each file containing the subscription data of one or more NPA-NXXs.

R8-6 The periodic interval for placing copies of the subscription data at the secure sites, and the number of NPA-NXXs in a single subscription data file shall be controlled by a tunable parameter.

8.3 NPAC/SMS Verify of Data in Local SMS

R8-7 The NPAC/SMS will be able to request data from the local SMS's for a given TN or a range of TNs. The request may be for all data for a TN or for specific fields.

R8-8 For audit requests from the NPAC/SMS to a local SMS, the size of the range of TNs will be limited by a tunable parameter.

R8-9 Both the SOA, via the NPAC/SMS to SOA interface, and the NPAC personnel shall be able to request data from one, some or all local SMSs, supported by the NPAC/SMS.

R8-10 The NPAC/SMS shall issue queries to each local SMS whose data is being verified.

R8-11 The NPAC/SMS shall compare the data received from each local SMS and take corrective action as appropriate for the following conditions:

a) Local SMS has incorrect data for a TN

b) Local SMS has TNs no longer ported, i.e. not active in NPAC/SMS

c) Local SMS does not have TN that is active in the NPAC/SMS

R8-12 The NPAC/SMS shall provide a final audit report to the requester indicating the results of the audit request.

R8-13 The NPAC/SMS shall permit providers to specify for their local SMS interface which, if any, SOAs they will accept audit requests from.

Section 9: Report Management

Overview

The NPAC and the NPAC/SMS shall have both defined and variable reporting capability.

R9-1 The NPAC shall be capable of generating ad hoc/free format reports and predefined reports. Such reports shall be available on-line or in hard-copy at the user's option.

R9-2 The NPAC/SMS shall support all report requirements defined in Section 9 of the FRS.

9.1 Informational Reports

R9-~~2~~3 The NPAC and NPAC/SMS shall be capable of producing, upon request, the following informational reports:

(a) reports on ported DN data (keyed on one or multiple fields for a single number or a range of numbers),

(b) reports on non-proprietary user data (keyed on one or multiple fields for a single user or a range of users),

(c) reports on the NPAC and NPAC/SMS performance (including CPU usage, number of transactions, mean time to complete broadcasts, and user link utilization), and

(d) reports as may be required by regulatory agencies.

R9-~~3~~4 For an interim period, the NPAC/SMS shall generate a report of portable NXXs. The NPAC/SMS shall also notify all users of new portable NXXs immediately upon notification by a service provider of a new portable NXX.

R9-~~4~~5 The NPAC is responsible for the accuracy of all informational reports.

9.2 Logs

R9-~~5~~6 The NPAC/SMS shall maintain complete and accurate logs of all transactions performed by the NPAC/SMS (including transactions requested by the NPAC).

R9-~~6~~7 Each log shall contain sufficient detail to record the following information for each transaction: purpose or type of transaction, date, time, requesting entity, information received or provided, direction of data flow, and disposition of request.

R9-~~7~~8 The NPAC/SMS shall be capable of retrieving the information in a log within 24 hours for logs less than two years old. Logs between two years and five years old shall be archived and retrievable within 7 days. Logs greater than 5 years old need not be maintained.

9.3 Repair Audits

R9-~~8~~9 The NPAC/SMS shall be capable of performing audits of NPAC/SMS data base, data link, and service provider data integrity at the request of a user for the purpose of troubleshooting a user problem and maintenance.

R9-~~9~~10 Authorized users shall have the ability to request that an audit be performed for (a) a ported DN or group of ported DNs; (b) a selected user s data link integrity; or (c) a selected user's network data.

R9-1~~0~~1 The audit reports generated shall contain sufficient information to provide the requesting entity with any and all information necessary.

Section 10: NPAC/SMS Reliability, Availability, Performance and Capacity

This section defines the reliability, availability, performance and capacity requirements for the NPAC/SMS.

10.1 Availability and Reliability

The NPAC/SMS will be designed for high reliability, including disaster recovery, and data integrity features, symmetrical multi-processing capability, and allow for economical and efficient system expansion. The system will adhere to the following availability and reliability requirements:

R10-1 It will be available 24 hours a day, 7 days a week. Describe the manner in which this availability will be achieved.

R10-2 It's reliability will be 99.9%. This applies to all functionality and data integrity. Describe the minimum, maximum, and average level of reliability provided.

R10-3 The amount of unscheduled downtime per year will be <= 9 hours. Describe in detail the manner in which this will be accomplished. In addition, provide the minimum, maximum, and the average amount of unscheduled downtime per year.

R10-4 For unscheduled downtime, the mean time to restore functionality will be <= 1 hour. Provide a description of types of failures and provide the minimum, maximum, and mean time to repair for each type of failure handled.

R10-5 The amount of scheduled downtime per year will be <= 24 hours. Describe in detail the manner in which the scheduled downtime is distributed.

R10-6 It will be capable of monitoring the status of all of its communication links and be capable of detecting and reporting link failures.

R10-7 It will be capable of detecting and correcting single bit errors during data transmission between hardware components (both internal and external).

R10-8 If a failure occurs resulting in downtime of any functionality, affected transactions received immediately prior to the failure must be queued and processed when functionality resumes. This may require real time updates to the backup system.

R10-9 The design will provide:

- Functional components with on board automatic self checking logic for immediate fault locating.

- Continuous hardware checking without any performance penalty or service degradation.
- Duplexing of all major hardware components for continuous operation in the event of a system hardware failure.
- Primary Vendors are required to clearly articulate in their responses their specific solutions for managing any downtime experienced by the NPAC/SMS.
- Primary Vendors are required to provide an inquiry capability (toll free number access and voice response units) for affected customers checking the outage status.

R10-10 If the system becomes unavailable for normal operations due to any reason, including both scheduled and unscheduled maintenance, service providers must be notified of the system unavailability.

- When possible, the notification will be made via an electronic broadcast message to the service providers. When this is not possible, the NPAC will notify the service providers via their contact numbers.
- The notification will include, at a minimum, the functionality that is unavailable, the reason for the downtime, estimated length of the downtime and a NPAC contact number.

R10-11 During any maintenance, if resources allow only partial functionality, the capability of receiving, processing and broadcasting updates will be given the highest priority.

R10-12 It must provide system tolerance to communication link outages and offer alternate routing during such outages.

R10-13 For any downtime, either scheduled or unscheduled, lasting more than 1 hour, the NPAC/SMS will switch service providers to a proposed "backup" or disaster recovery process as described in section 2. In most cases, the time to switch the service providers to another process and provide full functionality must not exceed the mean time to repair. However, in the event of a disaster that limits both the NPAC and NPAC/SMS's ability to function:

- The capability of receiving, processing and broadcasting updates must be restored within 24 hours.
- Full functionality must be restored within 48 hours.

The vendor is requested to describe the architecture used to satisfy the reliability and availability requirements, including the use, if any, of a "backup" and/or disaster recovery system/process and the use of any alternate disaster recovery location. Alternatives to the "backup" and disaster recovery process flow in Section 2 should be included here as well. Primary Vendors are required to

clearly articulate in their responses their specific solution for managing any downtime experienced by the NPAC/SMS.

R10-14 The vendor shall deliver the following documents/reports:

- Reports documenting the performance of the NPAC/SMS in regards to the above requirements will be provided periodically to the service providers.
- Perform and document a business impact analysis. This will among other things, determine the maximum tolerance period to the service providers and affected customers and ~~t~~business losses. The time allowed to resynchronize databases will be calculated as part of the tolerance period.
- Perform and document risk/threat analysis
- Document solution selection process
- Document business case for funding approval for recommended solution
- Document disaster recovery plan in terms of:
  - Hardware
  - Application
  - Operating system
  - Network
  - Human Resources
  - Emergency preparedness
  - Business resumption planning
  - Etc.

R10-15 The Primary Vendor shall schedule and perform disaster recovery exercises twice a year. During these exercises:

- Extract key learnings
- Upgrade disaster recovery plan and process before next exercise, if appropriate

10.2 Capacity and Performance

The following requirements define the capacity and performance of the NPAC/SMS. While the initial transaction rates and data storage requirements are not high, the NPAC/SMS is expected to provide high performance and allow for future expansion. Refer to section 13 for future expansion possibilities.

R10-16 The system will be engineered to allow for 75 service providers having SOA and SMS interfaces. Initially it is expected there will be approximately 25 service providers having SOA and SMS interfaces.

R10-17 Describe any capacity requirements related to any load generated by the NPAC personnel who will be users of the NPAC/SMS.

R10-18 The NPAC/SMS will be capable of handling transactions required for 30% above the following forecasts for ported numbers and churn rate. This is a median forecast and is not intended to reflect any participant's market penetration forecast. Churn is the percent of already ported numbers being moved

(and is assumed to be 30% each year).

The NPAC/SMS will be capable of handling the following number of transactions. Each record added or updated involves 1 transaction from the old service provider, 2 from the new service provider, and a broadcast to all service providers. For the purpose of this table, the number of service providers was assumed to be 75 (each year).

Year	Total Number of Lines (M)	% Portable	Subject to Porting (M)	% Pene-tration	Total Number of Transactions (M)
1998	25.8	60	15.5	10	140
1999	26.6	90	23.9	15	140
2000	27.4	95	26.0	20	180
2001	28.2	98	27.6	25	220
2002	29.0	98	28.5	30	250

The number of updates due to mass changes and the number of report requests is not known at this time.

R10-19 The ~~cumulativ~~number of on-line archived record requirements are shown in the table below~~:~~ (see R9-7).

Year	Archived Records (in Millions)
1998	1.8
1999	3.6
2000	4.2
2001	5.1
2002	6.1

R10-20 Data storage of the History file must keep track of all transactions made for one year (churn and new records). It is assumed that there will be thirty percent churn of accumulated records.

R10-21 From the time an activation notice is received from the new service provider to broadcast out an update until the time the update is broadcasted to all service providers will be < 60 seconds.

R10-22 The response time from when a request or transaction is received in the system to the time an acknowledgment is sent will be < 3 seconds. This does not include the transmission time across the interface to the service provider's SOA or SMS.

R10-23 The NPAC/SMS must be expandable to handle any future growth due to circumstances described in section 13.

Section 11: Billing / Resource Accounting

Resource Accounting allows the tracking of NPAC resource usage data, which may be used as a basis for billing the service providers for their use of NPAC functionality. Resource Accounting is responsible for gathering the information into usage measurement categories, aggregating the measurements, and formatting and outputting the measurements to the appropriate entities (e.g., Billing Operations Applications, service providers). Other potential applications for usage information include cost allocation, marketing, and usage studies.

R11-1 The NPAC/SMS shall maintain sufficient measuring and recording capability to produce an accurate bill to users.

R11-2 Billing reports for a particular user may be based on any combination of the following:

(a) duration, date/time, service provider ID, user login ID, of login session;

(b) number of transactions processed;

(c) number of updates made (by type);

(d) number of errors encountered in transactions;

(e) number of errors encountered during transmission;

(f) number of pending records maintained;

(g) number of active records maintained;

(h) number of archived records maintained;

(i) number of records downloaded as normal action;

(j) number of records sent in response to a resend request;

(k) number of records resent due to transmission problems;

(l) number of records in conflict;

(m) number of records audited on request;

(n) number of records corrected (e.g., as result of audit);

(o) number of records queried/viewed;

(p) amount of data transported to user SMS as bulk load update; CPU usage; and

(q) failures and maintenance problems in the NPAC/SMS.

R11-3 The billing reports from the NPAC and the NPAC/SMS must contain sufficient information to allow for each billed user to audit such reports.

Section 12: Number Portability Administration Center

12.1 Overview of the Role of the NPAC and NPAC/SMS

The NPAC/SMS is a hardware and software platform which contains the database of information required to effect the porting of telephone numbers in an LRN architecture. The NPAC/SMS shall not be involved in actual call routing, but rather shall receive, store, broadcast data on ported directory numbers ("DNs"), and provide informational reports based on the information contained in the database. This information is necessary to allow each user's network to properly route calls.

The NPAC shall manage the NPAC/SMS database. The NPAC shall be responsible for the maintenance and performance of the NPAC/SMS.

12.2 User Support and User Training

The NPAC shall be responsible for user support as required. Specifically, the NPAC shall (a) provide appropriate training for users; (b) provide technical support for users; and (c) perform both initial and ongoing acceptance testing for any and all functionalities.

R12-1 The NPAC shall be responsible for initial and ongoing training and user support.

R12-2 The NPAC shall train users, upon request, to:

(a) upload ported DN data and user data,

(b) receive and understand broadcasts,

(c) receive and understand error/success messages,

(d) request, receive, and understand mass changes,

(e) request, receive, and understand reports (including billing), and

(f) understand security measures.

R12-3 The NPAC shall provide technical support for users who experience problems in:

(a) uploading ported DN data and user data;

(b) receiving and understanding broadcasts;

(c) receiving and understanding error/success messages;

(d) requesting, receiving, and understanding mass changes;

(e) requesting, receiving, and understanding reports (including billing); and

(f) understanding security measures.

R12-4 The NPAC shall provide the necessary technical support to correct any data transmission problems encountered in the interfaces between the NPAC/SMS and a user.

12.3 Acceptance Testing

R12-5 The NPAC shall perform acceptance testing of the initial software and hardware configurations in the NPAC/SMS.

R12-6 The NPAC shall perform acceptance testing of all modifications or upgrades to software and hardware configurations in the NPAC/SMS. This software and hardware testing shall be scheduled so as not to inhibit the ongoing functionality of the NPAC/SMS.

R12-7 The NPAC shall resolve all problems encountered during testing.

R12-8 The NPAC shall document all testing procedures and test results and shall make those results available to users.

R12-9 The NPAC shall certify all NPAC/SMS software and hardware configurations before release for operation.

12.4 Geographic Requirements

While the NPAC need not be physically in the state of California, at least two Points of Presence (POPs) within the state must be provided for interconnection by users. The two required POPs shall be distant one from the other by at least 300 statute miles, distant one from the other far enough to not be significantly affected by the same catastrophic event (the risk analysis will indicate the distance). The intent of this requirement is to provide at least one POP in what is commonly referred to as Northern California, and one POP in what is commonly referred to as Southern California.

R12-10 There shall be at least two NPAC/SMS POPs in California, physically separated by at least 300 statute miles. It is recommended that these POPs NOT be located IN a large metropolitan area.

R12-11 The Primary Vendor shall be responsible for the facilities cost between the POP and the NPAC/SMS locations.

R12-12 The Primary Vendor shall define the locations of each POP and its actual facility.

R12-13 The NPAC/SMS shall support direct transmission facility connections from a service provider to each NPAC/SMS location. In this instance, the service provider will be responsible for the facilities' cost to the NPAC/SMS.

Section 13: Future Considerations

The future of number portability, such as the number of service providers and possible expansion to geographic and service portability, and number administration are not known at this time. The SMS platform should not preclude future expansion to adapt to additional needs as they arise.

Specifically, the following expected expansion is known at this time:

1. Expansion for use by Commercial Mobile Radio Services (CMRS) providers. This may require new data fields and expansion of service providers using the SMS. CMRS providers covered under the FCC Report and Order include cellular, broadband PCS, and covered SMR (Specialized Mobile Radio). It has not yet been determined what additional data field elements there will be for a wireless subscriber with a ported telephone number. Potential additional requirements beyond those already identified for a ported subscriber could be an STP, SCP, MSC address for message routing to the Home Location Register (HLR) and/or possibly a non-dialable mobile station identification (MSCID) which could be a 10-digit or a 15-digit format number. These are only possibilities and is not an all inclusive list. SMS requirements for covered CMRS providers will be determined by the wireless industry through appropriate industry activities and made available upon determination.

Other impacts that may occur are as follows:

1. Expansion to allow additional service providers. This will increase the number of ports needed for the links and the number of service providers sending updates and receiving broadcasts.
2. Expansion to other states: This will require an increase in the size of the database, and an increase in both the number of updates and the number of broadcasts. The number of service providers using the SMS may also increase. This may also require additional POPs.
3. Geographic number portability: This will require an increase in the size of the database, and an increase in both the number of updates and the number of broadcasts. There may also be interfaces between regional SMSs. Geographic portability may be done in stages, such as initially being geographic portability beyond current rate centers but within a specific region.
4. Pooled NXXs: This will require an increase in the size of the database due to all numbers within a shared NXX being in the database, and an increase in both the number of updates and the number of broadcasts. This may also require some number administration in the SMS.

5. Overlays of NPA-NXXs: The NPAC/SMS will be required to adapt to changes, if any, resulting from overlays.
6. Expansion to include data related to resellers. This may require data indicating the reseller, if any for telephone numbers and will increase the size of the database. Resellers may also need to access the database.

The above are not intended as requirements on the SMS, but only as information on possible future needs. Vendors are requested to describe how the NPAC and SMS can be adapted to accommodate the above situations. This information does not imply future obligation on the group to contract with the selected vendor for any future needs.

Section 14: Glossary

Activation Time Stamp	Date/Time Stamp of when the TN porting activation command was received by the NPAC/SMS from the new Service Provider. This time stamp is also stored in the Local SMSs and SCPs to assist auditing.
Auditing	Comparing of records in various systems to check for consistency and to correct any discrepancies. NPAC/SMS Local Service Provider network audit: comparing records stored in the NPAC/SMS and the Local Service Provider network.
Churn	Percent of ported numbers undergoing additional porting.
Disconnect Date	Date current Service Provider establishes intercept of a customer's service.
Due Date	The Due Date is a date/time stamp on a subscription order that indicates the approximate date/time of activation. The actual activation of the subscription order is triggered by the Activation Request from the new SP. The Due Date will be used to determine when both new and old SPs should have sent their matching subscription orders, as well as for aging old unprocessed orders from the system.
Effective Date	Date NPAC/SMS removes number from the database; the effective release date.
GTT	Global Title Translation - performed for CLASS and LIDB access features. A 10-digit GTT is now required for LNP (instead of the current 6-digit). This requires that the NPAC maintain: a) the DPC and ~~DPC type (End-office or Gateway)~~SSN information for the CLASS feature, and b) the DPC and SSN information for LIDB Gateway for LIDB access. c) the DPC and SSN information for Calling Name Delivery d) the DPC and SSN information for ISVM.
NPAC	Number Portability Administration Center is operated by a neutral third party, and performs administration functions for LNP.

NPAC/SMS	The regional SMS is the HW/SW platform for an Operations Support System that performs administration functions for the Local Number Portability Service. It is the master database for ported TNs.
LNP	Local Number Portability is the ability to port TNs. There are three flavors: • Service Provider Portability • Location (Geographic) Portability • Service Portability
Local SMS	The SMS used by the Service Provider, that receives LNP data from the NPAC/SMS and distributes it to the SPs network elements (e.g., SCPs). This is a logical function and may be implemented as a separate system or as part of a network element.
Longitude & Latitude	Coordinates to define geographic location for billing and rating purposes.
LRN	Location Routing Number is a 10-digit number used to uniquely identify a switch that supports porting.
Ported TN	A TN ported to a switch that is not the NANP-assigned switch.
Rate Center	Geographic locations assigned V & H coordinates between which distances are determined for billing and rating purposes.
Service Portability	The ability to port TNs when changing services, e.g., from POTS to ISDN.
Service Provider	A Service Provider that provides telecommunication services. Some examples of service providers are: • Local Service Provider • Long Distance Service Provider • SCP/SMS Service Provider • Directory Services/Operator Service Provider • Non-facilities-based Service Provider (e.g., Reseller)
Service Provider Portability	The ability to port TNs when changing service among Local Service Providers.
Subscription	Information record for a TN.

TN	Telephone Number
V&H Coordinates	Vertical and Horizontal Coordinates to define geographic location for billing and rating purposes.
Version	Time-sensitive (or status-sensitive) instance of subscription data.

Section 15: Acronyms and Abbreviations

AIN	Advanced Intelligent Network
CLASS	Custom Local Area Signaling System
DPC	Destination Point Code
FRS	Functional Requirements Specification
GDMO	Generalized Definitions of Managed Objects
GTT	Global Title Translation
IIS	Interoperable Interface Specification
IN	Intelligent Network
ISVM	Interswitch Voice Messaging
LATA	Local Access Transport Area
LIDB	Line Information Database
LNP	Local Number Portability
LRN	Location Routing Number
NANP	North American Numbering Plan
NPAC	Number Portability Administration Center
OCN	Operating Company Number
PPP	Point to Point Protocol
SOA	Service Order Activation
SMS	Service Management System
SP	Service Provider
SSN	Subsystem Number
TN	Telephone Number
TT	Translation Type

Section 16 Key Business Terms and Conditions

KEY BUSINESS TERMS AND CONDITIONS ACCEPTED BY PRIMARY VENDORS

1. _____ WCPS, shall have the right to terminate the Contractual Agreement entered into through this RFP with the Primary Vendor for reasons of default (including, but not limited to, unauthorized assignment of agreement and failure to provide adequate Service), upon 30 days notice. WCPS can avail itself of this termination option by at least a simple majority vote of its membership. Also, the Primary Vendor is forbidden from making any unilateral changes to the Master or Service Contracts entered into under this RFP.

2. _____ WCPS shall be granted appropriate license rights in and to any technology or other intellectual property that is developed for and at the request of WCPS for the purposes of providing the services; and Primary Vendor and Sub-Contractor(s), if any, shall agree to appropriate limitations on their use of any such technology or other intellectual property for purposes other than the express provision of the services.

3. _____ The Primary Vendor and Sub-Contractor(s), if any, shall deposit all technology and other intellectual property and related documentation under its control, that is necessary to the provision of these Services, with a mutually agreeable escrow agent for the use of WCPS, or to allow another vendor the ability to provide services, in the event of supplier default (e.g., bankruptcy, failure to perform, etc.).

4. _____ The Primary Vendor and Sub-Contractor(s), if any, agrees to indemnify and save harmless WCPS, its Members and their parents, subsidiaries, other affiliates, their direct and indirect customers, and the officers, directors, employees, successors, agents, representatives, successors and assigns of any and all of them (all hereinafter referred to in this clause as the "WCPS") from and against any and all claims, losses, damages, expenses, liabilities, suits, demands, causes of action, including costs and reasonable attorney's fees, or liens that arise out of or result from:

> (i) Injury or death to persons, or loss or damage to any and all property, including theft, in any way arising directly or indirectly out of, or occasioned by, caused or alleged to have been caused by, or on account of, the performance of the Work or Services performed by Primary Vendor, or Sub-contractor(s), if any, or its agents, or any director, officer, employee, agent or representative under this RFP, the Master Contract or the Services Contract (the Agreements),
>
> (ii) Assertions under Workers' Compensation or similar acts made by persons furnished by Primary Vendor, or Sub-Contractor(s), if any, or by reason of any injuries to such

persons for which WCPS would be responsible under workers' compensation or similar acts if the persons were employed by WCPS,

(iii) Any failure on the part of Primary Vendor, or Sub-Contractor(s), if any, to satisfy all claims for labor, equipment, materials and other obligations relating to the performance of the Work under the Agreements, and;

(iv) Any failure by Primary Vendor, or Sub-Contractor(s), if any, to perform its obligations under this clause, clause 9 (relating to insurance), or any clause in the Agreements.

The Primary Vendor shall defend or settle, at its own expense, any action or suit against the other for which it is responsible under the Agreements and shall reimburse the indemnified party for reasonable attorneys' fees, interest, costs of suit and all other expenses incurred by the indemnified party in connection therewith. The indemnified party shall notify the Primary Vendor promptly of any claim for which the Primary Vendor is responsible under this clause, and shall cooperate with the Primary Vendor in every reasonable way to facilitate the defense of any such claim.

5. _____ The Primary Vendor and Sub-Contractor(s), if any, shall be willing, at WCPS's request, to obtain a bid and/or performance bond in an amount sufficient to guarantee performance of its obligation under this RFP.

6. _____ The Primary Vendor and Sub-Contractor(s), if any, shall treat all information obtained from WCPS or its Members as confidential and proprietary unless they can demonstrate that such information was previously known by the Primary Vendor (or any sub-contractor, as applicable) without an obligation of confidentiality.

7. _____ No information furnished by the Primary Vendor or Sub-Contractor(s), if any, in response to this RFP or under any Contractual Agreement arising out of this RFP shall be considered confidential or proprietary, except the Tab 3, Cost and Price information described in Section 1.4.3.2.

8. _____ The Primary Vendor and Sub-Contractor(s), if any, will defend or settle, at its own expense, any claim or suit against WCPS alleging that any products or services furnished under the Agreements infringe any United States patent or copyright. The Primary Vendor will also pay all damages and costs that by final judgment may be assessed against WCPS due to such infringement. WCPS shall promptly notify the Primary Vendor of any claim, and shall cooperate with the Primary Vendor to facilitate the settlement or defense.

If any Primary Vendor products or services become, or in WCPS's opinion are likely to become, the subject of a claim of infringement, the Primary Vendor will, at its option: (1) procure for

WCPS the right to continue using the applicable product or service; or (2) replace or modify the product or service to provide WCPS with a non-infringing product or service that is functionally equivalent in all material respects.

9. _____ During the term of this Agreement, the Primary Vendor and Sub-Contractor(s), if any, shall obtain and maintain, with financially reputable insurers (i.e., carriers with an A.M. Best rating of B+:VII, or better) which are licensed to do business in all jurisdictions where any work is performed and which are reasonably acceptable to WCPS, not less than the following levels of insurance coverage:

a.) Worker's Compensation as provided for under any worker's compensation or similar law in any jurisdiction where any work is performed, with an employer's liability limit of not less than $500,000 per accident or disease;

b.) Commercial General Liability, including coverage for Contractual Liability and Products/Completed Operations Liability, with a limit of not less than $1,000,000 combined single limit per occurrence for bodily injury, property damage and personal injury liability (with contractual exclusion deleted), naming WCPS, its members, their directors, officers, employees, agents and/or representatives as additional insureds;

c.) Business Auto insurance covering the ownership, maintenance or use of any owned, non-owned or hired automobiles with a limit of not less than $1,000,000 combined single limit per accident for bodily injury and property damage liability, naming WCPS, its members, their directors, officers, employees, agents and/or representatives as additional insureds;

d.) Umbrella/Excess liability with limits of not less than $9,000,000 combined single limit in excess of the above-referenced Employer's Liability, Commercial General Liability and Business Auto liability coverage naming WCPS, its members, their directors, officers, employees, agents and/or representatives as additional insureds;

e.) "All Risk" Property insurance covering not less than the full replacement cost of Primary Vendor's and any Sub-Contractor(s), if any, personal property at risk due to this Agreement; and,

f.) Errors and Omissions insurance in the amount of at least $1,000,000 per claim with an annual aggregate of at least $3,000,000 inclusive of legal defense costs.

Waiver of Subrogation: Primary Vendor shall look first to any insurance in its favor before making any claim against WCPS, its members, their directors, officers, employees, agents and/or representatives for recovery resulting from injury to any person (including Primary Vendor's or Sub-Contractor's employees, if any) or damage to any property

arising from any cause, regardless of negligence, and does hereby release and waive to the fullest extent permitted by law, and shall cause its insurers to waive, all rights of recovery against WCPS, its members, their directors, officers, employees, agents and/or representatives.

Certificates of Insurance: Primary Vendor and Sub-Contractors, if any, must, as a material condition of this Agreement, prior to the commencement of any work and prior to the renewal thereof, deliver to WCPS a certificate of insurance, satisfactory in form and content to WCPS, evidencing that the above insurance is in force and contains a provision that it will not be canceled or materially altered without first giving WCPS thirty (30) days prior written notice and that all coverage is primary to any insurance carried by WCPS or its members.

Nothing contained in this section shall limit Primary Vendor or Sub-Contractor's, if any, liability to WCPS or its members to the limits of insurance coverage certified or actually carried.

10.) _____ The Primary Vendor shall submit a list of Sub-Contractor(s), if any, to WCPS with its Qualification submission, for review and approval. Any subsequent change in the use of any Sub-Contractor(s) shall require the review and approval of WCPS.

11.) _____ The Primary Vendor and Sub-Contractor(s), if any, shall not have the right to assignment of the Contractual Agreement entered into through this RFP without the prior approval of WCPS.

12.) _____ The governing law under this RFP and any Contractual Agreement entered into through this RFP shall be that of the state of California.

13.) _____ In the event that the Service does not pass a mutually agreed upon Acceptance Plan, designed to determine the Primary Vendor's system compliance with the functional and technical requirements of this RFP, WCPS shall have the option to terminate the arrangement without any penalties whatsoever to it or its member carriers.

Section 17 Process Flows

California LNP OPI Team
DRAFT Version 1.0 9/16/96

Time Legend

t_1 = Period the NPAC will wait for the second create/change request after receipt of the first.

t_2 = The agreed to time between Old and New Service Provider.

t_3 = Period the NPAC will wait for the second cancellation request after receipt of the first.

t_4 = Period the NPAC allows for conflict resolution to occur before it cancels the order.

t_5 = Period the NPAC will wait for activation after receiving confirming order from second Service Provider.

California LNP OPI Team
DRAFT Version 1.0 9/16/96

Provision Service Process Flow
(3 day overall time frame suggested)

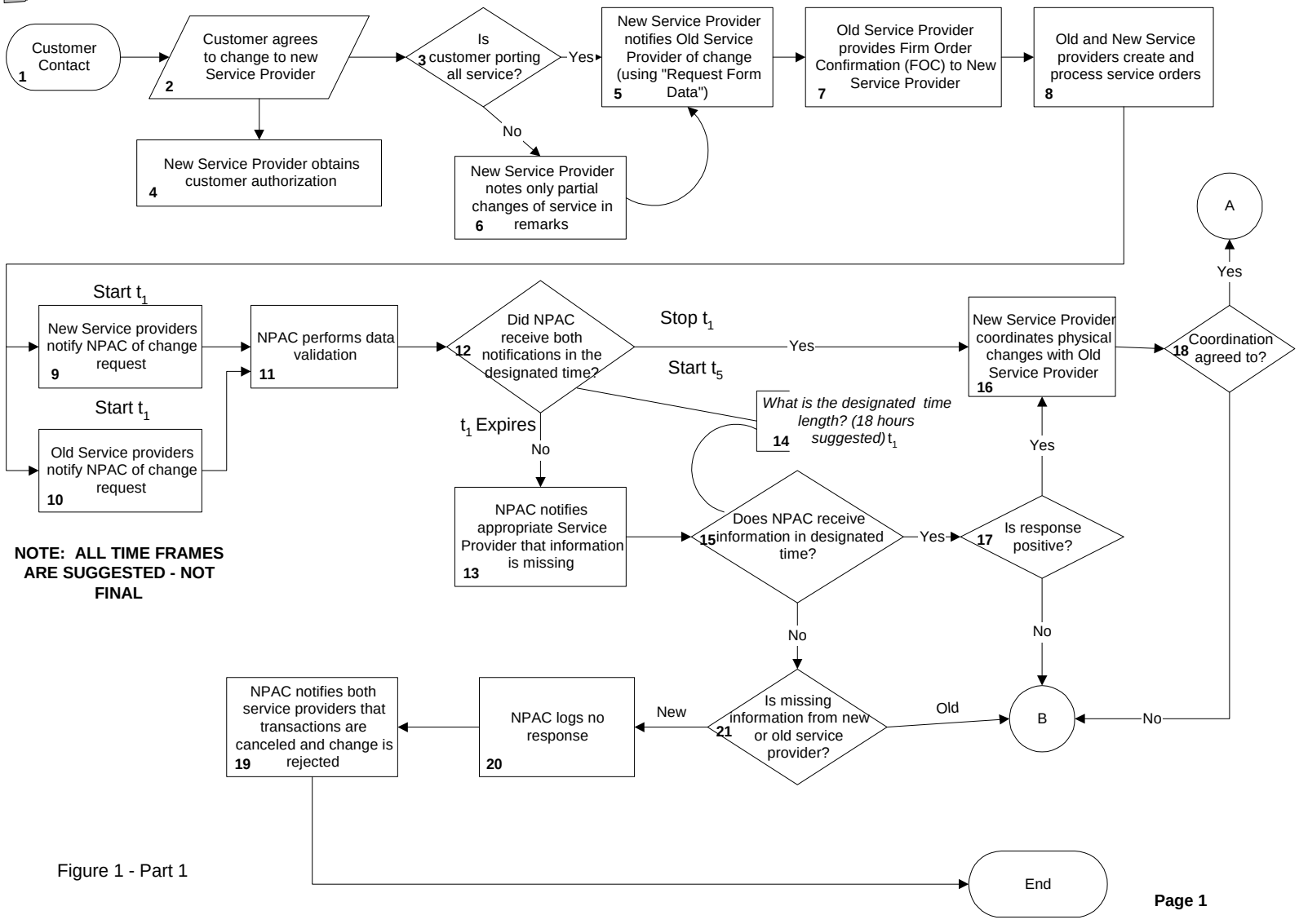


Figure 1 - Part 1

California LNP OPI Team
DRAFT Version 1.0 9/16/96

Provision Service Process Flow

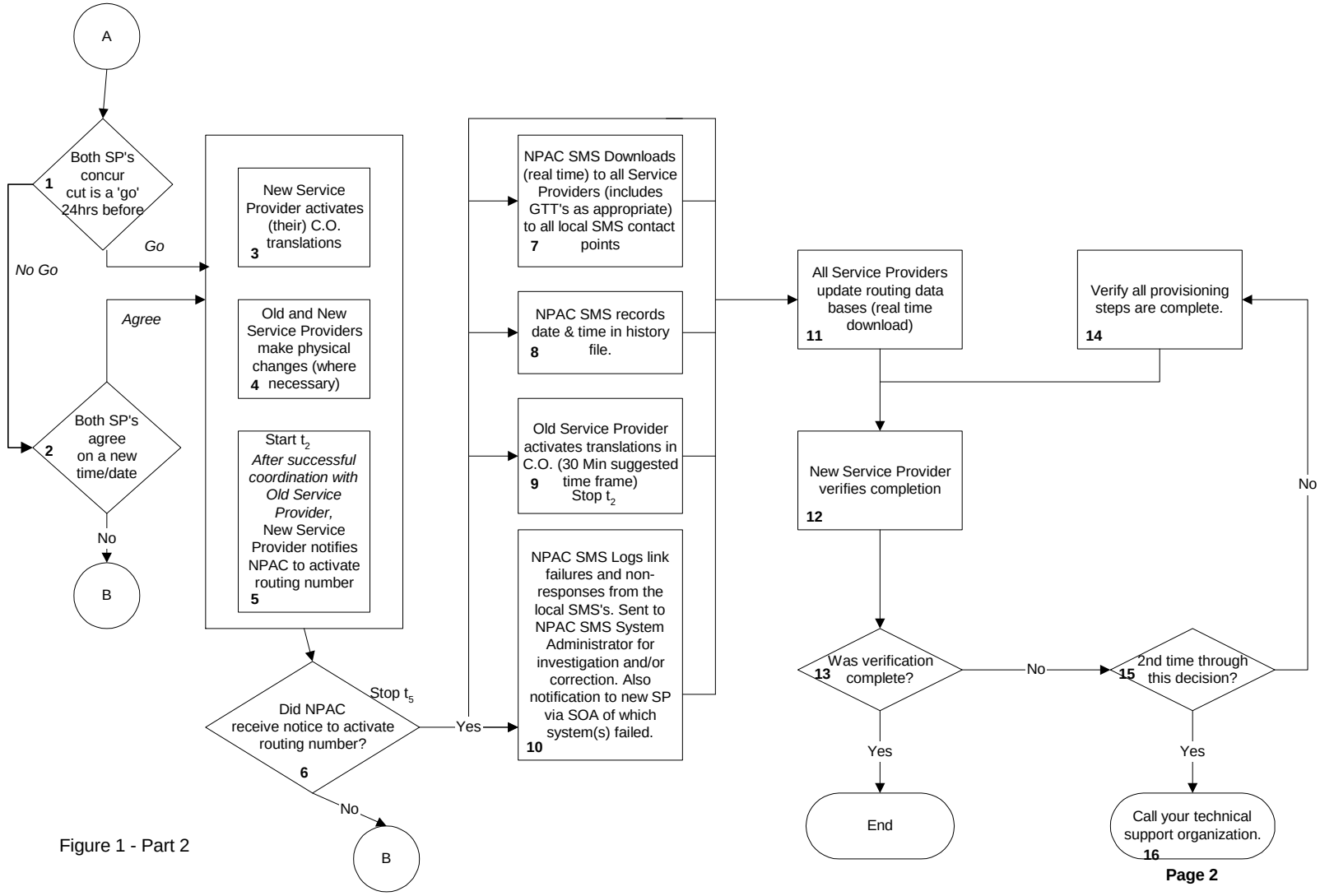
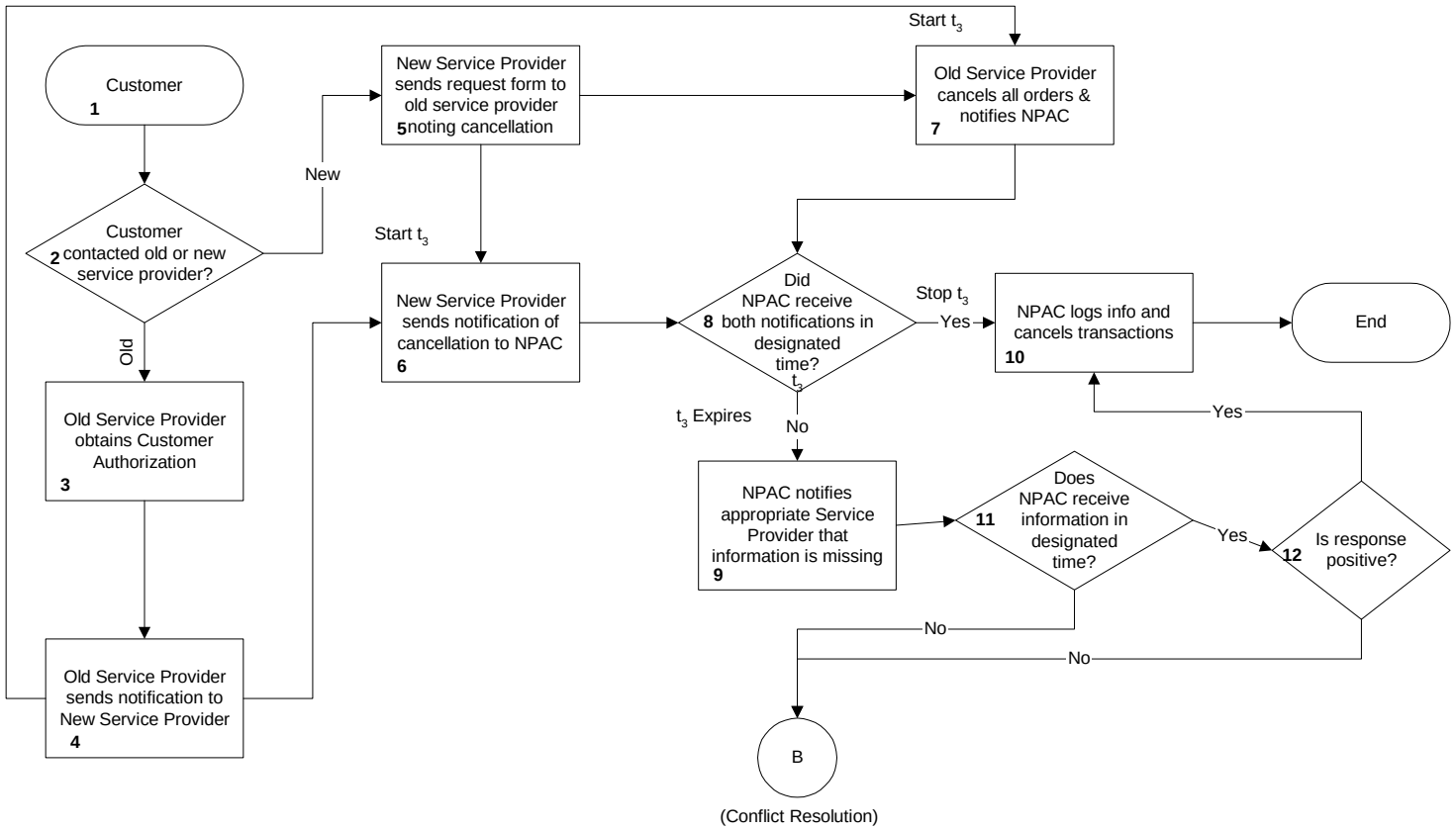


Figure 1 - Part 2

California LNP OPI Team
DRAFT Version 1.0 9/16/96

Provision Service Process Flow
(Cancellation of Service Order)



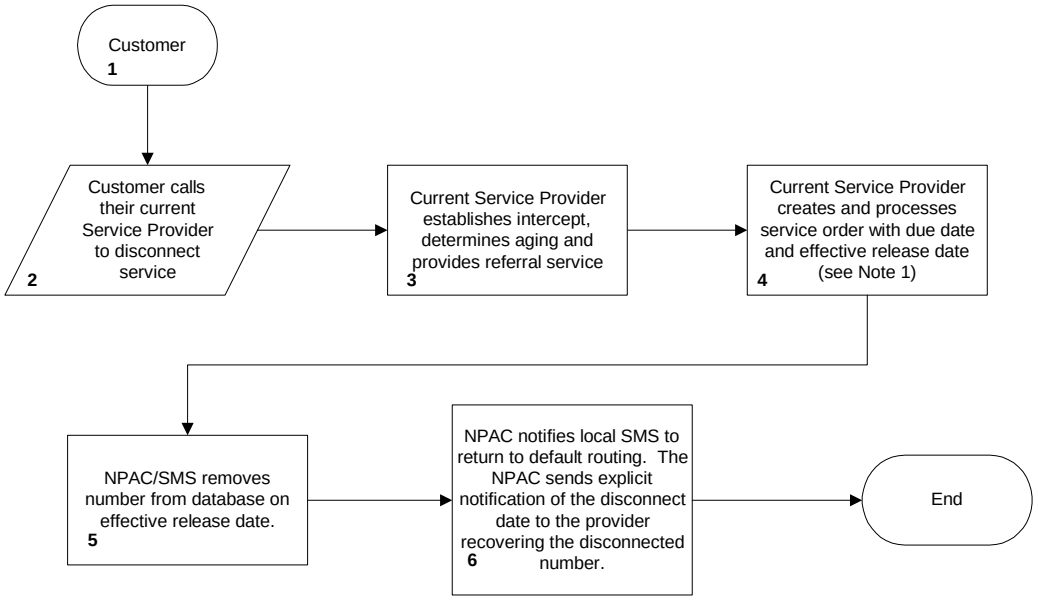
****** Note Suggested NPAC Designated Time = 18 Hrs.***

Figure 2

California LNP OPI Team
DRAFT Version 1.0 9/16/96

Disconnect Service for Ported Number

No explicit notification of a disconnected number will be given to the original donor by the NPAC

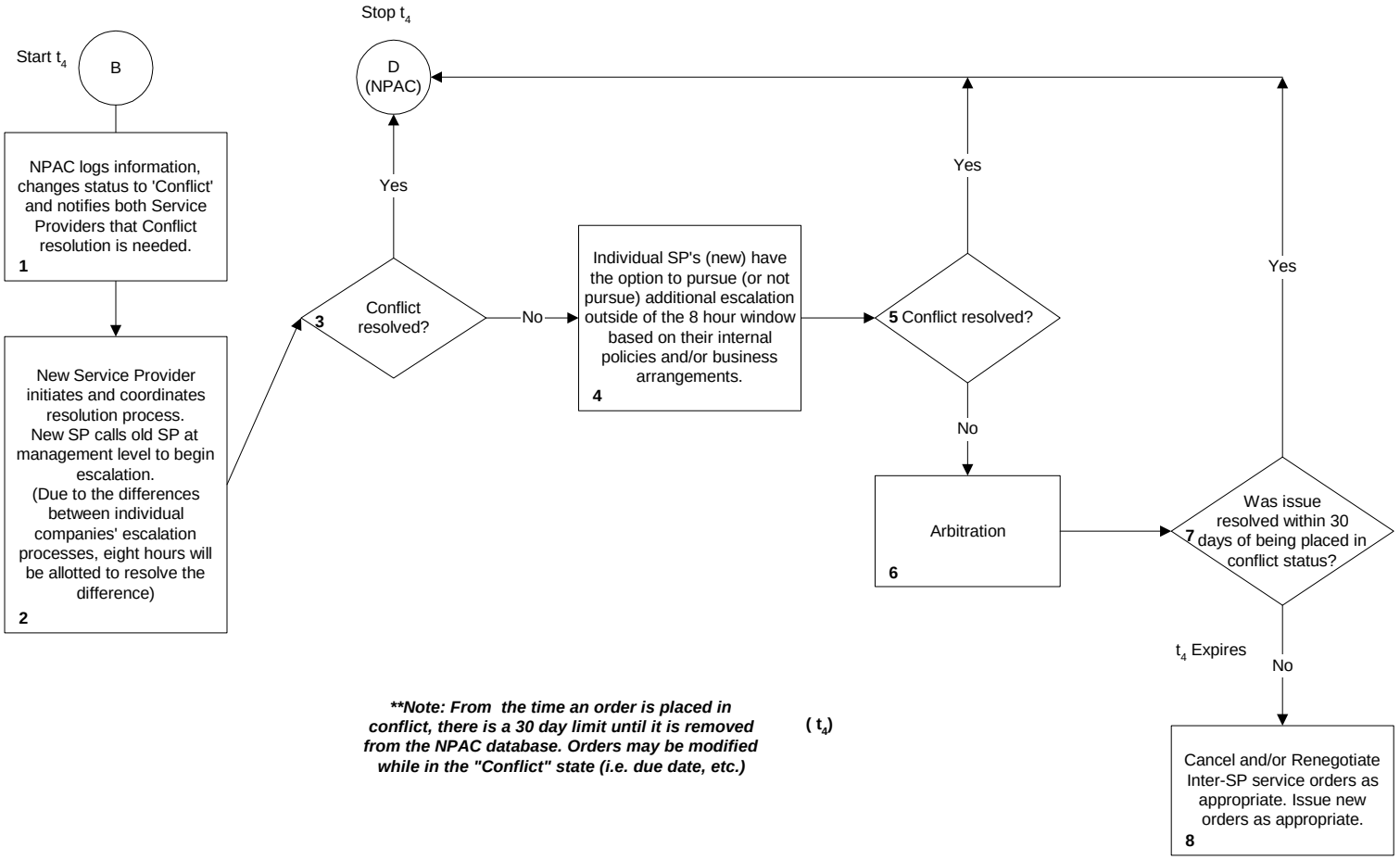


**** Note 1: If no effective release date is given the default will be immediate***

Figure 3

California LNP OPI Team
DRAFT Version 1.0 9/16/96

Conflict Resolution - Part 1 of 2



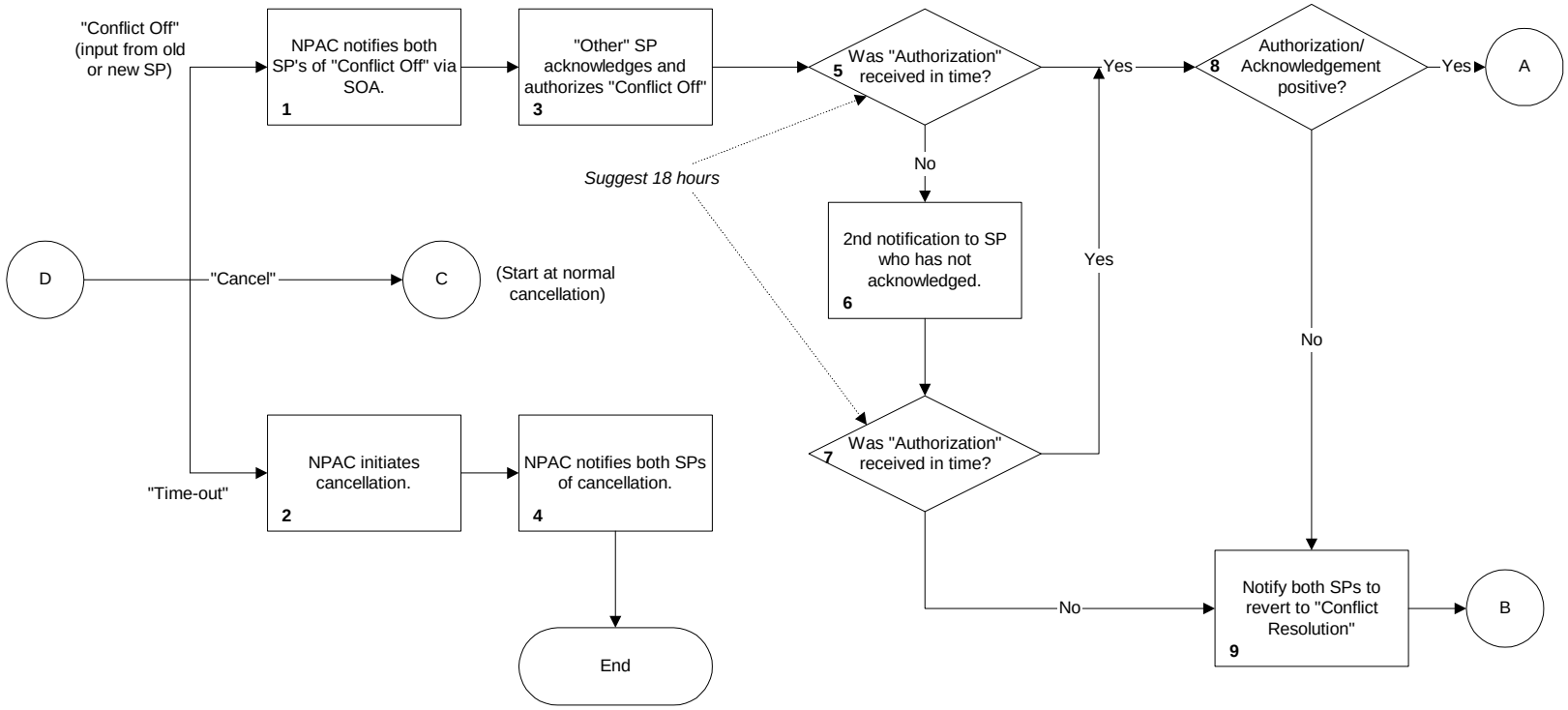
Note: From the time an order is placed in conflict, there is a 30 day limit until it is removed from the NPAC database. Orders may be modified while in the "Conflict" state (i.e. due date, etc.)

(t_4)

Figure 4 - Part 1

California LNP OPI Team
DRAFT Version 1.0 9/16/96

Conflict Resolution - Part 2 of 2



***Note: 30 day "Time-out" begins when order is placed in conflict. Without positive notification of resolution, the NPAC initiates cancellation at the end of 30 days.*

Figure 4 - Part 2

Attachment 2

SECTION 1: GENERAL INFORMATION

1.1 Introduction

1.1.1 Purpose of Request for Proposal

The purpose of this Request for Proposal (RFP) is to invite you to participate in submitting a total solution and associated firm pricing proposal to provide a Number Portability Administration Center and Service Management System (NPAC/SMS) to support the implementation of Local Number Portability in the Chicago LATA 358 in the state of Illinois. Your response should be based upon the specifications provided in this RFP and should contain detailed information on degree of compliance to requirements, pricing and availability.

The Selection Committee consisting of Ameritech, AT&T Corp., TCG, MCI Metro, Sprint/Centel and MFS will evaluate all proposals from a total network and operations perspective to ensure integration with existing network and operating procedures. Proposals will also be assessed on their ability to evolve, as necessary, from serving a limited geographic area to a nationwide service and with minimal obsolescence of existing investment.

Prospective vendors may be required to furnish components of their systems to the Selection Committee for evaluation and testing and/or to make arrangements on their own premises for facilitating joint testing, at no charge.

1.1.2 Use of RFP Information

You shall use this RFP and any other information furnished to you under this RFP solely for the purposes of responding to this RFP. All such documents and information you receive shall remain the property of the Selection Committee, shall be kept confidential and shall be returned to the Selection Committee upon request. Reproduction of any part of this RFP is authorized only for the preparation of your response. You shall not disclose this RFP to any of your employees who do not have a "need to know" or to any third party working with or for you without the prior written consent of the Selection Committee. You shall ensure that all such copies (both paper and computer form) are destroyed when no longer required in connection with this RFP.

1.1.3 Vendor's Information

Do not submit any proprietary or confidential information or mark it as such. Information furnished by you to the Selection Committee pursuant to this RFP shall not be considered by you to be confidential or proprietary. In no event will the Selection Committee consider or hold any information contained in your proposal proprietary or confidential, except for pricing information.

1.1.4 Background

1.1.4.1 History of LNP Activities in Illinois to Date

An industry task force was formed in Illinois in April 1995, pursuant to the Illinois Commerce Commission (ICC) Order on Customers First Plan (Docket 94-0096 dated April 7, 1995), to develop a permanent number portability solution for Illinois. During the year, this task force has made significant progress in defining and resolving the issues related to implementing number portability. Among other things, the task force has determined that:

-Initially, only wireline service provider portability within existing LEC rate centers will be implemented.

- The long-term architecture for routing calls will be Location Routing Number (LRN).

- The target date for LRN implementation is second quarter 1997.

Consistent with the timetable, it is the intention of the task force to select an NPAC/SMS vendor on or about the end of the first quarter 1996, start system testing in the fourth quarter 1996, with projected full functional operability in the second quarter 1997.

1.1.4.2 Impact of Federal Regulation and Legislation on this Procurement

This RFP is being issued by a group of service providers who currently provide or intend to provide facilities-based local exchange services in the state of Illinois. LNP implementation is subject to oversight by the Illinois Commerce Commission (ICC). However, bidders should be aware that the Federal government, through Congressional legislation, Federal Communications Commission rule making, or other mandates, may establish policies for local competition which may affect the operation of the NPAC.

1.2 Description of LNP Environment

1.2.1 LNPArchitecture
The Illinois Local Number Portability task force has selected the Location Routing Number (LRN) architecture to enable the correct routing of calls in this number portability environment. A high-level description of the LRN architecture is presented in Section 16, Figure 5 (Part 1 and 2).

1.2.2 Functions of the SMS
The Service Management System is a hardware and software platform which contains the database of information required to effect the porting of telephone numbers. In general, the SMS receives customer information from both the old and new service providers (including the new Location Routing Number), validates the information received, and downloads the new routing information when a "activate" message is received indicating that the customer has been physically connected to the new service provider's network The SMS also

contains a record of all ported numbers and a history file of all transactions relating to the porting of a number. The SMS shall also provide audit functionality and the ability to retransmit LNP information to service providers under certain conditions. The SMS is not involved in real time call processing.

1.2.3 Management and Integration Role of NPAC

The NPAC shall provide management oversight for and integration of the data center operations and software development and maintenance functions. It shall have responsibility for achieving performance standards established by the industry and for providing user and technical support services and training for industry participants.

1.3 Eligibility to Submit Proposals

1.3.1 Prime Vendor

NPAC/SMS business shall be awarded to a single Prime Vendor who shall be responsible for providing a total solution encompassing the NPAC functionality and the SMS platform (both hardware and software). The Prime Vendor shall be responsible for all NPAC administration duties and system performance adherence in accordance with the requirements of this RFP. The Prime Vendor shall be the single point of contact for the Contracting Entity. The Prime Vendor shall be required to submit a comprehensive proposal to provide all elements of the solution. At its option, the Prime Vendor may use its own resources exclusively or engage the services of subcontractors to provide one or more elements of the SMS platform (hardware, software, etc.) or other elements of the total solution.

1.3.2 Neutral Third Party

NPAC/SMS business shall be awarded to a Prime Vendor and/or NPAC administrator who is a "neutral third party." A neutral third party is an entity which:

l) is not a telecommunications service provider. A telecommunications service provider is an entity which provides, for generally-available public use, the transmission of information by electromagnetic or optical means;

2) is not owned by, or does not own, any telecommunications service provider. Ownership interests of five percent (5%) or less shall not be considered ownership for purposes of this section;

3) is not affiliated, by common ownership or otherwise, with a telecommunications service provider.

1 .3.3 Subcontractors

Responses to this RFP shall clearly state the roles and responsibilities of any and all subcontractors which are providing parts of the total solution under the direction of the Prime Vendor.

1.3.4 Additional Qualifications

1.3.4.1 General Background of Bidder(s)
RFP responses shall contain a concise description of the principal business of the Prime Vendor and any subcontractors, including such items as company background, characteristics of business strength, performance support for a multiyear business award, accomplishments and capabilities which demonstrate a strong foundation for managing and operating the NPAC, policies and procedures that will ensure evenhanded treatment of all carriers, and certification that the Prime Vendor and any subcontractor shall comply with the provisions of this Section.

1.3 .4.2 Industry Experience
RFP proposals shall include a concise description of the telecommunications experience of the Prime Vendor and any subcontractors, including such items as products and services offered, customers served, successful performance of the functional skills required by this RFP on activities performed for other customers, and customer benefits that resulted from such successful performance.

1.3.4.3 Financial Stability
RFP proposals shall include a concise description of the financial condition of the Prime Vendor and any subcontractors. Responses should include the most recent annual report or audited financial statement of the Prime Vendor and any subcontractors. Proposals shall include all characteristics of bidder(s) financial strength to support a multi-year business award.

1.4 Preparation of Responses

1.4.1 Proposal Submission
Your proposal, complete in all respects, must be submitted to the following address:
M. Gary Berg
2000 West Ameritech Center Drive
4C87A
Hoffman Estates, IL 60196-1025
Your cover letter should include both the name(s) and phone number(s) of the individual(s) within your company who should be contacted in case any questions should arise during the evaluation of your proposal.

Please give written notice of your interest to respond as soon as possible to the above address, **but no later than February 12, 1996.** If you would like to validate your neutrality status as a Prime Vendor please submit this request at the same time and you will be notified within ten working days. This validation will not impact the timeframe for response to this RFP. In addition, upon receipt of your interest to bid, a sample contract will be provided.

Failure to direct your response to the address given above by the noted closing date may result in the disqualification of your proposal.

The package containing your proposal shall be marked "Sealed Proposal" with this RFP title and your company's name.

1.4.2 Closing Date

All proposals in response to this RFP shall be received NO LATER THAN 12:00 Noon (Central Standard Time), **March 18, 1996.**

1.4.3 Response Composition

You shall submit seven (7) sets (hard copy and diskette copy in IBM DOS format, Word 5.0/ Excel 4.0) of copies of your proposal. Please mark all pages of one (1) paper copy "Master Copy". If discrepancies between copies and/or the diskette are found, the "Master Copy" will govern.

Your proposal shall be typed double spaced on 8-1/2" x 11" 3-hole punched paper with each volume beginning on a new page and separately tabbed.

You are requested not to make your proposal elaborate with respect to binding or presentation. A simple, straightforward. economically reproduced proposal is strongly recommended. Our proposal evaluation procedure places a higher premium on thoroughness of presentation, i.e., responsiveness, rather than on quantity of material included.

1.4.4 Questions or Requests for Additional Information

Submit your question(s) or request(s) for additional information in writing to the following facsimile number listed below no later than **February 22, 1996** prior to the closing date for this RFP.

847 248-3284
ATTN: M. Gary Berg

All questions and responses shall be promptly distributed to all recipients of this RFP. Please note that the identity of the requesting company shall be withheld. Telephone inquiries will not be accommodated.

1.4.5 Acceptance Period

Your proposal shall indicate that it is valid for a period of at least one hundred eighty (180) days from the closing date.

1.4.6 Contract Award
The contracting entity or entities of the Selection Committee reserve the right:
a) to reject any and all responses:
b) to conduct negotiations with more than one vendor simultaneously
c) to add, delete and/or change the terms of this RFP and to issue corrections and amendments to the RFP
d) to accept or reject, in whole or in part, any response without giving any reason for the decision

e) to enter into a contractual arrangement with any vendor and is not limited by any event associated with this RFP

f) to have any documents submitted by a vendor reviewed and evaluated by any individuals, including, independent consultants;

and
g) to cancel the RFP process without penalty at any time before a written contract is entered into.

1.4.7 No contractual obligations are assumed by issuing the RFP, receiving, accepting, and evaluating the vendor's response, and/or making a preliminary vendor seleciion.

1.4.8 The Selection Committee reserves the right to cancel any agreement if the services or facilities do not pass mutually agreeable acceptance tests. This will be done at no cost or obligation to the Selection Committee contracting entity or entities.

1.4.9 The Selection Cornmittee contracting entity or entities reserve the right to negotiate all terms and conditions in order to enter into a formal agreement with the successful vendor. This document, the vendor's response, and full system documentation will form part of the agreement.

1.4.10 No publicity or news releases pertaining to this RFP, responses to this RFP, discussions of any kind regarding the RFP, or the award of any agreement related to the bid document may be released without the prior written approval of the Selection Committee.

1.4.11 All work and materials must comply with all federal and state law, municipal ordinances, regulations, and directions of inspectors appointed by proper authorities having jurisdiction.

1.4.12 The vendor shall not assign, transfer, or sublet the RFP service agreement or any interest therein or any part thereof without prior written consent. All subcontractors must be identified and approved prior to disclosure of any information. If subcontracting is involved, the primary vendor shall be responsible for the workmanship, costs, etc. Incurred by the sub-contractor in the performance of their duties.

1.4.13 The vendor, by stating compliance to a requirement in this RFP, agrees that the vendor has read and understood the requirement and that compliance is complete and deliverable at no additional cost unless otherwise noted.

1.4.14 This RFP may include unintended errors, omissions, and/or deficiencies. Therefore, the accuracy and completeness of this document and related documents are not guaranteed. In the event that such errors, omissions, and/or deficiencies are discovered by the vendor, the vendor shall notify the Selection Committee in writing within 48 hours.

The vendor is expected to examine the specifications and instructions carefully. Calculation errors shall be the vendor's risk. In the event of a vendor's error in price, time or calculations, quoted items shall prevail.

1.5 Additional Contractual Terms and Conditions This section identifies contractual terms and conditions that the contracting entity intends to incorporate into the Agreement. The following list is in addition to the terms and conditions specified in the RFP.

1. Conformity with Law Vendor shall comply with all applicable FCC rules and federal, state, and local statutes, regulations and case law.
2. Indemnification Vendor shall provide indemnification with regard to damage, death, or personal injury due to vendor's acts or omissions.

3. Trademarks and Publicity

Vendors shall have no rights to use names or trademarks.

4. Confidentiality Vendor shall not disclose confidential information.

5. Termination The Agreement shall establish the right of termination without liability if vendor substantially defaults in performing obligations.

6. Limitation of Liability Except specifically provided in the Agreement, there shall be no liability for vendor's damages.

7. Taxes Vendors shall file all tax returns required by law to be filed by vendor: vendor shall provide access to relevant documents for tax audits.
8. Insurance Vendor shall maintain worker's compensation insurance, employer's liability insurance, comprehensive general liability insurance, and motor vehicle insurance.
9 Authonty Vendor shall represent and warrant that vendor has approval and authority to execute the Agreement.
10. Mechanic's Lien Vendor shall perform services free of mechanic's lien or other liens.

1.6 Preparation of Proposal Response

1.6.1 Content Structure You are responsible for any and all costs incurred in the preparation of your response to this RFP. Your proposal shall consist of the following separate Tabs: Tab 1 Proposal Summary Tab 2 Functional and Technical Requirements Tab 3 Cost and Price

DO NOT INCLUDE COST OR PRICE FIGURES ANYWHERE EXCEPT IN YOUR TAB 3 RESPONSE, THE COST AND PRICE SECTION.

All proposals meeting the stated requirements and specifications except for minor exceptions and deviations, shall be considered. Failure to meet requirements may disqualify a proposal from the selection process. However, proposals having minor exceptions and deviations shall be considered only if the following conditions are satisfied: (a) all exceptions and deviations from the specifications are explicitly stated in the Proposal Summary; and (b) all exceptions and deviations are appropriately justified on the basis of performance, schedule and/or relative price.

1.6.2 Tab Content

The required content of each tab of your proposal follows:

Proposal Summary (TAB 1)

This tab should summarize all key features of your proposal response. All deviations and exceptions from the RFP should be stated, and a brief justification given. A more detailed justification can be included in the tab that covers the subject.

Functional and Technical Requirements (TAB 2)

This section should discuss the major aspects of the functional design. You should address

(1) all areas which result in a potentially high degree of risk
(2) all areas which impose an unusually high degree of responsiveness, and

(3) areas that are deficient and that could be improved.

Cost and Price (TAB 3)

This tab shall include a description of the proposed costs and prices. All pricing information shall be limited solely to this tab of your proposal. For purposes of your response you should provide both a three year and five year view. (See Section 10, R10-17 and 18) This tab should address all requirements set forth in this RFP as well as any other items pertinent to your proposal pricing such as additional discounts for increased volume, prompt payment, transportation charges (FOB destination)etc. Pricing shall also be firm for all orders place through December 31, 2001, and shall be based on the EF&I of all applicable goods, software, and services of the most recent vintage and/or technology available in the telecommunications industry.

1.7 Evaluation of Proposals

The criteria to be used for the proposal evaluation include:
(a) technical merit
(b) schedule
(c) price and cost
(d) quality considerations
(e) responsiveness to contract provisions

(f) Prime's financial stability, history, including program management

No weighting or relative importance of criteria is intended or implied by this list.

You shall furnish all information as requested per the applicable instructions providing sufficient data to enable us to evaluate the proposal. Any deviations or exceptions to the RFP should be noted. Any supplier who does not completely reply to the proposal as requested may be eliminated at the discretion of Selection Committee.

The same article, section or paragraph number and title used in the RFP shall be used for your comments.

In the cases where your reply is "will not be complied with" or "not agreed to", you shall indicate your reasons for such disagreement and provide an alternative with which you will comply or agree.

SECTION 2: BUSINESS PROCESS FLOWS

The following process flows indicate how the NPAC and NPAC/SMS are used in the various business processes associated with number portability. This information is intended to provide an overview of the role of the SMS in number portability. Details of steps in the processes that do not involve the NPAC or NPAC SMS, such as interactions between service providers, will be determined by the service providers and are beyond the scope of this document. Specific requirements generated by the process flows are included in the appropriate sections later in the document.

2.1 **Provision Service Process**

This process flow defines the provisioning flow in which a customer ports a telephone number to a new service provider.

The new service provider will obtain authorization to port the customer and notify the old service provider according to processes internal to the service providers. Both the old and new service providers will send a notification to the NPAC SMS from their Service Order Administration Systems. When the NPAC SMS receives the notification(s), it will perform certain validation checks, including that both the old and new service provider has sent a notification. If errors are found or both service providers did not send notifications, the SMS will enter into a coordination process described in the next paragraph. Assuming the notifications are valid, the two service providers will complete any physical changes required. At the time new service provider is ready to provide service, it will send an activation notice to the NPAC SMS. The NPAC SMS will place an activation time stamp on the update and broadcast the update out in real time to all local service providers' networks. Upon receiving the update from the NPAC SMS, all service providers will update their networks. The NPAC SMSwiU record any transmission failures and take the appropriate action.

In the case where either the old or new service providers did not send a notification to the NPAC SMS, the NPAC SMSwiU notify the service provider from which it did not receive a notification that it is expecting a notification. If it then receives the missing notification and the notifications indicate agreement among the service providers, the process proceeds as normal. If it still does not receive a notification and if it is the old service provider that failed to respond, the NPAC SMSwiU log the failure to respond and then the process proceeds as normal. If it was the new service provider that failed to respond, the NPAC will log the failure to respond, cancel the notification, and notify the old service provider of the cancellation. If there is disagreement among the service providers as to who will be providing service for the telephone number, the conflict resolution procedures will be implemented. Processes for obtaining authorization from the customer to port a number are defined by the service providers. The NPAC is not involved in obtaining or verifying authorization.

From the time the new service provider sends a notification to the time it sends the activation notice, the new service provider may send a message to the NPAC SMS to cancel the notification. If this occurs, the NPAC SMS will remove the notification from its database and notify the old service provider that the notification has been canceled.

(refer to Figure 1 in Attachments)

2.2 **Disconnect Process**

When a ported number is being disconnected, the customer and service provider will agree on a date. After an aging period, if any, the service provider will send an update indicating the disconnect to the NPAC SMS. The NPAC SMS will broadcast the update to all service providers and remove the telephone number from its database of ported numbers. Upon receiving the update, all service providers will remove the telephone number from their LNP databases. The NPAC SMS will log the update in history. Calls to the telephone number will be routed as a nonported number.

In both the service provisioning process and disconnect process, when the NPAC SMS is performing validity checks (such as confirming that required data fields are filled in), if an error is found, the NPAC SMS will notify the service provider's with an appropriate error message. The service provider will have to resend the notification to have it processed.
(refer to Figure 2 in Attachments)

2.3 Repair Service
A problem will be detected either by a service provider or by a customer contacting a service provida.

There will be audit capabilities in the NPAC SMS to aid in isolating problems. If an inaccuracy is found, the NPAC SMS will broadcast the correct data to any involved local service provider to correct inaccuracies.

(refer to Figure 3 in Attachments)

2.4 Conflict Resolution Process
If service providers disagree on who will serve a particular line number, the NPAC will place the request in "conflict" and notify both service providers. The service providers will determine who will serve the customer via internal processes. When a resolution is reached, the NPAC will be notified and will remove the request from "conflict" or cancd it.

2.5 **Disaster Recovery and Backup Process**
If there is planned downtime for the NPAC SMS, the NPAC SMS will send an electronic notification to the service provider's SOAs that includes information on when the downtime will start, how long it will be and if they will be required to switch to the backup or disaster recovery machine. Downtime is considered planned when the NPAC can provide notification to the service providers at least 24 hours in advance. If the downtime will be less than 60 minutes, the service providers will remain connected to the primary machine and not send any updates during the downtime. If the downtime will be longer than 60 minutes, the NPAC service providers will switch to the backup or disaster recovery machine as indicated in the notification. There will be a quiet period (minutes) when no updates can be sent in order to allow the NPAC to coMect the service providers to the proper machine. At the end of the quiet period, processes will proceed as normal. When the primary machine is brought back up, the backup or disaster recovery machine will send an electronic notification to the service providers' SOAs indicating the

time the NPAC will switch them back to the primary machine. At the end of the quiet period, processes will

continue as normal and the NPAC will synch up the database in its primary SMS with any updates sent to the backup or disaster recovery machine during the downtime.

If there is unplanned downtime, the NPAC will assess how long the primary machine will be down. The NPAC will notify all of the service providers by telephone calls to the service providers' contact numbers of the situation and planned action. If the downtime is expected to be less than 60 minutes, the service providers will remain connected to the primary machine and not send any updates during the downtime. If the downtime will be longer than 60 minutes, the service providers will switch to the backup or disaster recovery machine and later back to the primary using the same process as described for planned downtime. In addition, once the service providers have been switched off of the primary machine, each service provider will check to see if any updates of newly ported numbers sent to the primary machine during the time it went down were not broadcast out. If a service provider finds such updates, the service provider may use internal inter-carrier processes to update its own SCPs and have other carriers update their SCPs with the information in order to ensure service to the affected customers. This will not be needed for disconnect orders. Even if it finds such updates, a service provider may choose to wait until it can begin sending updates to the backup or disaster recovery machine and then just resend the updates that had died in the primary machine. If a service provider does use internal processes to request updates to SCPs while waiting to be able to send them to the backup or disaster recovery machine, the service provider will still resend the updates when backup or disaster recovery machine can begin processing them in order to ensure every service provider and the NPAC SMS receive the update.
(refer to Figure 4 in Attachments)

3.1 Overview The NPAC SMS manages the ported TN information associated with the service provider portability for the LNP service.

3.1.1 Service Data The Service Data contains global parameters specific to the LNP service. Examples of some of these parameters are described below. The description presents a logical representation of the data, not an implementation view. Time interval for concurrence from both service providers (Section 5, R5-21) Number of retries for download to Local SMS (Section 5, R5-59) Time interval a subscription version stays in conflict (Section 5, R5-44)

3.1.2 Service Provider Data Service Provider Data contains information about service providers participating in the LNP service. The data items that need to be administered by Service Provider Data Administration include (but are not limited to): A. Service Provider Name B. Facility-based Service Provider Identification C. Service Provider Address D. Service Provider Phone E. Service Provider Contact F. Service Provider Repair Center Information G. Service Provider System Data Link Information

3.1.3 Subscription Data Subscription Data consists of information about the ported TNs. The data items that need to be administered by Subscription Data Administration functions are described below. The description presents a logical representation of the data, not an implementation view. Table 3-1 describes the data items associated with each ported TN that are maintained by the NPAC SMS. Size of the data items is in bytes.

TABLE DID NOT SCAN

3.1.4 Network Data

The data items that need to be administered by Network Data Administration functions are described below. The description presents a logical representation of the data, not an implementation view.
A. Participating facilities-based service providers and their IDs
B. NPA-NXXs that are portable
C. LRNs associated with each facilities-based service provider
D. Service Provider valid Location Values
E. Valid Billing Ids

Certain types of updates made to network data, such as NPA splits, may cause mass changes to data managed by the NPAC. The NPAC will need to support such mass changes, which typically involve an investigation of all service, service provider, and subscription data in order to determine if such data will be affected by the change, as well as the potential modifications and activation of the data records affected by the change.

An NPA split is supported by maintaining two sets of records or an equivalent mapping to reduce memory costs and administrative care (old NPA and new NPA) in the NPAC SMS, Local SMSs, and SCPs for the duration of the permissible dialing period, during which dialing of both NPAs are allowed. After the expiration of the transition period, all records for the old NPA are removed from the systems.

3.2 NPAC Personnel Functionality
R3- l Authorized NPAC personnel shall be able to initialize the network data when the NPAC SMS is initially deployed.
R3-2 Authorized NPAC personnel shall be able to administer NPAC network data.
R3-3 Authorized NPAC personnel shall be able to open up a new NPA-NXX for LNP.
R3-4 Authorized NPAC personnel shall be able to add/delete a service provider.
R3-5 Authorized NPAC personnel shall be able to administer information related to a service provider.

R3-6 Authorized NPAC personnel shall be able to perform mass changes that affect several records. NPA splits, LRN changes, LIDB changes and other similar network data changes affect multiple subscription records in the NPAC SMS.
R3-7 Authorized NPAC personnel shall be able to select a subset of data which matches a user defined selection criteria, and specify a mass update action to be applied against all key data elements found in the selected records.

3.3 System Functionality
R3-8 The NPAC SMS shall support an off-line batch download (e.g., via tape) mechanism to mass update Local SMSs (e.g., for new service providers, or in case of disaster recovery for a Local SMS).

R3-9 The NPAC SMS shall be able to download network data (e.g. portable NPA-NXX data), to the Local SMSs.

R3- 10 The NPAC SMS shall notify (electronic bulletin) all service providers about the availability of the NPA-NXXs for porting. NOTE: This is a temporary solution.

R3- 1 1 The NPAC shall notify (broadcast / electronic bulletin) all service providers about a new service provider and the associated LRNs. NOTE: This is a temporary solution.

R3- 12 The NPAC shall validate the service, service provider, and subscription data against the current network data.

R3-13 The NPAC SMS shall have the capability to identify all records affected by mass changes, (such as NPA splits), and automatically carry out the required updates and download the modified data to the Local SMSs.

SECTION 4: SERVICE PROVIDER DATA ADMINISTRATION

4.1 Service Provider Data Administration and Management

Service Provider Data Administration functions allow NPAC personnel to receive and record data needed to identify authorized LNP service providers. The service provider data indicates who the LNP service providers are and includes location, contact name, security, routing, and network interface information. These functions will be accessible to authorized NPAC personnel.

Service Provider Administration supports functionality to manage service provider data. There can be only one instance of service provider data for a specific LNP service provider.

Service Provider Administration Requirements

4.1.1 User Functionality
Authorized NPAC personnel can invoke the following functionality in the SMS to administer service provider data:

R4- 1 Create a new service provider - creates, validates, and updates new service provider data.
R4-2 Modify service provider data - modifies, validates, and updates existing service provider data.
R4-3 Delete service provider data - deletes the service provider data and stores it in a history file.
R4-4 View service provider data.
R4-5 View a list of subscriptions associated with the service provider (i.e., see all ported INs associated with a specific service provider).
Additionally, authorized service provider personnel can view their own service provider data.

4.1.2 System Functionality
This section describes SMS functionality required to support the NPAC user requests described in the above section. The following specifies user requests and lists the SMS functionality needed to support those requests:

4.1.2.1 Service Provider Data Creation
An NPAC user requests that service provider data be Heated in SMS by associating an action of "aeate" with the data. This functionality enables a new instance of service provider data for a service provider be Heated, provided that no other service provider data exists for the service provider.

R4-6 When the NPAC user is creating a new service provider, SMS shall receive the following to identify the service provider:

R4-7Service Provider ID - identifier of the service provider (e.g., the OCN).
SMS shall check to see if there is an existing service provider with the same service provider ID. If there is, the SMS shall notify the user that the service provider data already exists for the service provider and that the new service provider data cannot be created.

R4-8 If there is no existing service provider data, the SMS shall receive the following data:

Service Provider name, address, phone number, and contact organization <-- required data:

Service Provider billing name, address, phone number, and billing contact for NPAC billing <-- optional data. If left blank this shall default to service provider name, address, phone number, and contact.

Service Provider to service provider Repair contact name and phone number <-- optional data. If left blank this shall default to service provider contact and phone number.

Location Routing Numbers (LRN) - the identifier of the switches having portable NXXs and used by the service providers <- at least one LRN is required.

Assigned NPA-NXXs open for LNP <-- at least one required.
Network Address of NPAC to Local SMS interface
Network Address of NPAC to SOA interface
Security data
R4-9 After the service provider data has been collected, SMS shall validate that all required data has been received as defined in R4-8.
R4- 10 If all validations are passed, SMS shall notify the user that the request to create the service provider data was successful.
R4- 11 If the service provider data fails validation, SMS shall issue an appropriate error message to the request originator. The service provider data shall not be created.

4.1.2.2 Service Provider Data Modification

An NPAC user requests that service provider data be modified in SMS by associating an action of "modify" with the service provider data. This functionality enables a user to add or change data for the service provider.

R4- 12 SMS shall receive a request to modify service provider data.
R4-13 SMS shall receive the following data from the user to identify the service provider data to be modified: the Service Provider ID.

R4-14 If the service provider data does not exist, SMS shall issue an appropriate error message to the request originator. SMS shall not proceed further with the modification request.

R4- 15 SMS shall allow all data to be modified or added to the service provider data with the exception of the SeNice Provider ID which is the key to the service provider data.

R4- 16 When a user attempts to submit modified service provider data, SMS shall revalidate the service provider data. This revalidation process shall include the validations defined in R4-9.

R4- 17 If the service provider data fails validation, SMS shall issue an appropriate error message to the request originator.
R4- 18 If the validations defined in R4-9 are passed, SMS shall determine if there are any subscriptions associated with the Service Provider ID.
(A) If there are no subscriptions, SMS shall notify the user that the request to modify the seNice provider data was successful, or
(B) If there are subscriptions that contain data that is dependent on the service provider data proposed for change, SMS shall notify the user that the request to modify the senice provider data cannot be completed until the individual subscriptions are modified via subscription administration functions.

4.1.2.3 Delete Senice Provider Data
When an NPAC user requests that senice provider data be deleted in SMS a network action of "delete" will be associated with the subscription data and it will be written to a history file.
R4- 19 SMS shall receive a request to delete service provider data.
R4-20 SMS shall receive the following data from the user to identify the seNice provider data to be deleted: the Senice Provider ID.
R4-21 If the service provider data does not exist, or if is has already been deleted and exists only in a history file, SMS shall generate an error message and send it to the request originator. SMS shall not proceed further with the deletion request.
R4-22 If the seNice provider data does exist, SMS shall do the following:

SMS determine if there are any subscriptions (i.e., ported TNs) associated with the service provider:
(A) If there are no subscriptions, SMS shall notify the user that the request to delete the seNice provider data was successful and shall write the service provider data to a history file which includes the date and time of deletion and the login of the NPAC personnel.

(B) If there are subscriptions, SMS shall notify the user that the request to delete the service provider data cannot be completed until the subscriptions are deleted or are associated with a different service provider.

4.1.3 Service Provider Queries

The query functionality discussed in this section will give users the ability to view service provider data without being able to update that data. A user may not be able to modify a particular data item because that user does not have the proper security permissions and the data is made available via SMS for read-only purposes.

Assumptions

Users will need to be able to retrieve service provider data that they cannot modify.

User Functionality

R4-23 An authorized SMS user shall be able to invoke the following functionality in the SMS to query service provider data: a service provider may view only its own service provider data. R4-24 Authorized NPAC personnel shall be able to view: all subscriptions associated with a service provider, or all subscriptions associated with a LRN.

System Functionality

The following specifies SMS functionality needed to support the user requests described above.

Service Provider Query

R4-25 For queries regarding service provider data, SMS shall receive the Service Provider ID.

R4-26 If SMS does not have service provider data as specified by the request originator, SMS shall provide the request originator with a message indicating that there was no data in SMS that matched the search keys. Otherwise SMS shall return all service provider data associated with the Service Provider ID.
R4-27 For queries regarding subscription data for a specific service provider, SMS shall receive the Service Provider ID, a request to view subscription data, and optionally the subscription data status types to be returned (e.g., active only, active or pending).

R4-28 If SMS does not have subscription data as specified by the request originator, SMS shall provide the request originator with a message indicating that there was no data in SMS that matched the search keys. Otherwise SMS shall return all subscription data associated with the Service Provider ID and any optional status requests.

Subscription List Ouery

R4-29 For queries regarding subscriptions, SMS shall receive the attributes to be searched on. Allowable attributes are all data elements in Table 3-1 or subsets thereof.

R4-30 If SMS does not have subscriptions as specified by the request originator, SMS shall provide the request originator with a message indicating that there was no data in SMS that matched the search keys. Otherwise, SMS shall return all subscriptions (active versions only) which satisfy the selection criteria. If more than a pre-specified number of subscriptions are found. (This shall be a parameter which is tuneable by the SMS System Administrator the default value shall be 50.) The subscription data shall be returned to a previously designated (off-line) output device/medium.

SECTION 5: SUBSCRIPTION ADMINISTRATION

5.1 Subscription Administration and Management

Subscription Administration functions allow users to specify data needed for ported numbers. The gubgenptian data indicates how local number portability should operate to meet subscribers' needs. These functions will be accessible to authorized service provides via an interface (e.g., the SOA interface) from their operations systems to the NPAC SMS and will also be accessible to (and performed by) NPAC personnel.

Subscription Administration supports functionality to manage multiple versions of subscription data. A subscription version can be associated with the following statuses: invalid, pending, sending, active, conflict, failed, canceled, or old (history). See Version Management for more details on different states of a version. There can be only one invalid, pending, sending, conflict, or failed version per subscription. There can also be one active subscription version at any time and multiple old and/or canceled subscription versions.

5.1.1 Version Management

Version management provides functionality to manage multiple time-sensitive views of subscription data. This sections addresses version management for LNP and the user and system functionality needed for subscription administration. In this context a version may be defined as time-sensitive subscription data.

At any given time, a subscription version in the SMS can have one of several statuses (e.g., active, invalid) and may change status depending on results of different SMS processes (e.g., modification, activation). This section describes different statuses that a version can have and the SMS processes that can change the status.

This section on Version Management discusses functionality and data that is needed for Subscription Administration.

Requirements

Version Status

R5- 1 At any given time, a version in the SMS will have one of the following statuses:

Pending - passed initial validations and edits and will be submitted to the network (i.e., Local LNP SMSs) when activation is requested.

Invalid - failed validations.

[Note: SMS will not create subscriptions or accept updates to subscriptions which result in an invalid condition. However, pending subscriptions will be revalidated prior to sending updates to the local SMSs. Subscriptions that fail this revalidation will have a status of invalid. It will be necessary to notify the porting service provider of this change in status.]

Conflict - non-concurrence from old facilities-based service provider, lack of concurrence from new facilities-based service provider, or dispute between two new facilities-based service providers. Sending - being sent to the network. Active - currently active in the network. Failed - failed activation in the network (at one or more Local SMSs). Old - previously active in the network. Canceled - previously pending, invalid, or in conflict.

The length of time that old subscription versions will be retained (before deletion) and will be accessible through a query request will be a tuneable pararneta that is tuneable by the SMS Administrator (with the appropriate security permission). The default value for this parameter will be eighteen (18) months.

R5-3 The length of time that canceled subscription versions will be retained (before deletion) and will be accessible through a query request will be a tuneable parameter that is tuneable by the SMS Administrator (with the appropriate security permission). For canceled versions, this parameter shall be tuneable based on the last status of the version. The default values for these parameters shall be as follows:

Last status before cancellation	Parameter value
pending	90 Days
invalid	90 Days
conflict	30 Days

Figure 5-1 illustrates the possible status transitions a subscription version may undergo.

Figure 5-1 Version Statuses

R5-4 The LNP SMS will maintain only a single pending version of a subscription.
R5-5 Subscriptions for individual ported TNs that are created through a "TN rangelevel" request shall be treated as individual subscription versions after activation has occurred.

R5-6 SMS shall log all subscription administration transactions. The log entries shall include: Activity Type: create, modify, active, activate, conflict "on," conflict "off," disconnect, cancel, or query Initial Version Status

New Version Status User ID and/or Login Local Number Portability Type (SP, Loc., Serv) Date and Time Starnp

Ported Telephone Nurnber

Status Flag - successful or failed

5.1.2 Subscription Administration Requirements

5.1.2.1 User Functionality

Authorized users2 can invoke the following functionality in the SMS to administer subscription data:
R5-7 Create a subscription version - creates, validates, and pends (if valid) a new subscription version for activation in the network.
R5-8 Modify a subscription version - modifies, validates, and pends (if valid) a pending, invalid, or active subscription version for activation in the network. Old, canceled, conflict, and failed versions cannot be modified.

R5-9 Activate a subscription version - activates a pending subscription version in the network.
R5- 10 Conflict "On"/Conflict "Off" - places a subscription version in conflict or removes it from conflict. A subscription version in conflict cannot be activated.
R5- 11 Disconnect a subscription version (from the network) - deletes the active subscription version in the network and stores it as an old subscription version.
R5- 12 Cancel a subscription version - removes an invalid, conflict or pending subscription version and stores it as a canceled subscription version.
R5-13 Query: displays a subscription version and its associated parameters.

5.1.2.2 System Functionality

This section describes SMS functionality required to support user requests defined in the above section. Subscription versions can be created or viewed by the old facilities-based service provider. Subscription versions can be created, modified, activated, disconnected, canceled, or viewed by the new facilities-based service provider. In addition to being able to create, modify, activate, disconnect, cancel, and view subscriptions, only authorized NPAC personnel can place subscriptions in conflict and remove them from conflict. Additionally, any authorized service provider can view any subscription version for any ported TN. (Note: Tuneable security permission matrix may be required.)
Additionally, SMS functionality is required to perform operations which are not invoked by a direct user request. This functionality shall monitor a subscription version to determine whether the old and the new facilities-based service providers have authorized the transfer of service for a ported number, shall issue appropriate notifiers to service providers, and shall change the status of a subscription version based on tuneable parameters, e.g. pending version will be automatically canceled after an "X" number of days ("X" = tuneable parameter)

2 An "authorized user" shall be able to access the data that is part of or controlled by the SMS. A user, either an individual or machine, shall be identified by a unique user identification code (user id).

The following specifies user requests and lists the SMS functionality needed to support those requests:

5.1.2.2.1 Subscription Version Creation

A user requests a subscription to be created in SMS by associating an action of "create" with a version. This functionality, which can be invoked by the old or the new facilities-based service provider, enables a new instance of a subscription version for the ported telephone number to be created, provided that there exists at most one active subscription version. Multiple old and/or canceled subscription versions may exist. If a create is initiated by the old facilities-based service provider, they shall identify the ported telephone number, the new facilities service provider, the due date and indicate that they are authorizing the transfer of service. If the create is initiated by the new facilities-based service provider, all information pertaining to the ported TN may be provided, with the exception of the old facilities-based service provider's authorization.

R5-14 When the user is the old (ported-from) service provider SMS shall receive the following to identify the subscription version to be created:

Local Number Portability Type IO - identifier of the Local Service Provider Portability (LSPP) type. (NOTE: While Local Service Provider Portability will be the first type supported by the NPAC SMS, the system needs to be extensible so as to support multiple types at a future date.)

Ported Telephone Number(s) - this entry can be a single TN or a continuous range of TNs that identifies a subscription or a group of subscriptions that share the same attributes.
Due Date - date on which transfer of service from old facilities-based service provider to new service provider is planned to occur.

New facilities-based service provider ID - the identifier of the new facilities-based service provider.

Old facilities-based service provider ID - the identifier of the old facilities-based service provider.

Authorization from old facilities-based service provida - indication that the transfer of service is authorized by the ported-from service provider.

R5-15 When the user is the new facilities-based service provida SMS shall receive the following to identify the subscription vasion to be created:

Local Number Portability Type ID - identifier of the Local Service Provider Portability type.

Ported Telephone Number (TN) - the identifier of a subscription (i.e., the telephone number assigned to the customer).

Due Date - date on which transfer of service from old facilities-based service provider to new facilities-based service provider is planned to occur.

New Facilities-based Service Provider ID - the identifier of the new facilities-based service provider.

Old Facilities-based Service Provider ID - the identifier of the old facilities-based service provider.

Authorization from New Facilities-Based service provider - indication of whether the transfer of service is authorized by the new Facilities-based service provider.

Location Routing Number (LRN) - the identifier of the ported-to switch.

LIDB Global Title Translation (GTT) data - network addressing information for routing to the serving LIDB.

Destination Point Code (DPC) type for LIDB features GTT indicates whether destination point code identifies the subsystem or a gateway STP.

CLASS Global Title Translation (GTT) data for LIDB DPC network addressing information (i.e., mapping of new LRN to destination point code) for routing TCAP messages to the ported-to switch.

Destination Point Code (DPC) type for CLASS features GTT indicates whether destination point code identifies the end of fice or a gateway STP.

R5-16 The following fields are for future use. The new facilities-based service provider may not be required to treat these fields as mandatory.

Billing Service Provider ID
End-User Location - Value
End-User Location - Type
Future 1
Future 2
Future 3

SMS shall invoke the following Version Creation functionality:
R5-17 When a user attempts to submit a new version, SMS shall determine whether a pending version already exist for the entity in question.

If a pending version exists and if the authorized user is associated with the old or new facilities-based service provider (who has not yet authorized the transfer of service), SMS shall:

Allow the old facilities-based service provider to perform the functions defined in R5-14 or
Allow the new facilities-based service provider to perform the functions defined in R5-15 and R5-16.

Otherwise, the SMS will send an error message to the request originator.

R5-18 If there is no pending version of the subscription (or if the conditions in R5-17 have been met) and no active version, SMS shall proceed as follows:

SMS shall perform the following validations for the version: All data has been received as defined in R5-14 or R5-15 and R5-16. The old and the new facilities-based service provider must agree as to the Due Date. The Due Date is the current date or a future date.

The NPA-N~ of the ported Telephone Number must be in the Portable NPA-NXX table. The old and new facilities-based service provider IDs must match existing service provider data.

The new LRN must be associated with the new facilities-based service provider. The LIDB DPC data must be associated with the new facilities-based service provider.
. .

The CLASS DPC data must be associated with the new facilitiesbased service provider.

R5-19 If there is no pending version of the subscription but there is an active version, SMS shall, in addition to the validations defined in R5- 16, verify that the old service provider on the version being created is equal to the service provider on the active subscription version.

R5-20 If the subscription version fails validation, SMS shall issue an appropriate error message to the request originator. If a valid subscription version already exists (e.g., the current create is being done by the old facilities-based service provider, but the new facilities-based service provider has already done a create for the ported TN), the pending subscription version shall be retained. Otherwise, the subscription version shall not be created.

R5-21 If the subscription version passes validations, SMS shall:

Verify if both the old and the new facilities-based service providers have authorized the transfer of service for the ported TN.

If not, SMS shall compute the date by which authorization data from both service providers must be received and shall store this with the subscription version. The date by which concurrence from both service providers must be received shall be computed as being a predetermined number of days prior to the Due Date. This will be a parameter that is tuneable by the SMS Administrator. The default value for this parameter shall be three (3) days.

Mark the version with a status of pending in the SMS and issue an appropriate message to the request originator indicating successful completion of the pending process.

R5-22 When the date for concurrence for a pending subscription version has been reached, SMS will send a notifier to the service provider (old or new) who has not yet authorized the transfer of service.

R5-23 If authorization for the transfer of service has not been received from the new facilities-based service provider within the allotted period of time (tuneable parameter) after SMS sent the notifier, the subscription version shall be canceled as defined in R5-70. The user ID for this transaction shall be the "SMS System ID."

5.1.2.2.2 Subscription Version Modification

A user requests a pending, invalid or conflict subscription version to be modified in SMS by associating an action of "modify" with a version. This functionality, which can be invoked only by the new facilities-based service provider, enables a user to add or change data in a subscription version.

5.1.2.2.2.1 Modification of a Pending, Invalid, or Conflict Subscription Version

R5-24 SMS shall receive data in support of modification of a subscription version:

(1) to change the data associated with a pending, conflict, or invalid subscription version or (2) to add additional data to a pending or conflict subscription version.

R5-25 If the version status is sending, failed, canceled, or old, SMS shall generate an error message and send it to the request originator. SMS shall not proceed further with the modification request.

R5-26 SMS shall receive the following data from the user to identify the subscription version to be modified: the Local Number Portability Service ID and the Ported Telephone Number Subscription ID.

R5-27 SMS shall allow the following data to be modified in the subscription version:

Location Routing Number (LRN) - the identifier of the switches having portable NXXs and used by the service providers <- at least one LRN is required.

Due Date - date on which transfer of service from old facilities-based service provider to new service provider is planned to occur.

LIDB GTT data - network addressing information for routing to serving LIDB.

DPC type for LIDB features GTT - indicates whether Destination Point Code identifies the subsystem or a gateway STP.

CLASS GTT data - network addressing information for routing TCAP messages to the ported-to switch.

DPC type for CLASS features GTT - indicates whether Destination Point Code identifies the end office or a gateway STP.

R5-28 The following fields are for future use. The new facilitiesbased service provider may not be required to treat these fields as mandatory.

Billing Service Provider ID

End-User Location - Value

End User Location - Type

Future 1

Future 2

Future 3

R5-29 SMS shall revalidate the modified subscription version. This revalidation process shall include the validations defined in R5-18.

R5-30 If the version fails validation, SMS shall issue an appropriate error message to the request originator. The pending subscription version, which the user was attempting to modify, shall be retained with no changes.

R5-3 1 If the version passes validations, SMS shall mark the version with a status of pending in the SMS and shall issue an appropriate message to both old and new service providers indicating successful completion of the pending process.

R5-32 If for a version that passed validations, the Due Date has been modified SMS shall send a notifier to the old facilitiesbased service provider informing them of the new Due date.

5.1.2 .2 .2 .2 Modificanon of an Acnve Subscripnon Version
R5-33 SMS shall receive data in support of modification of an active subscription version to change only specific data associated with an active subscription version.

R5-34 SMS shall invoke version creation functionality to create a new (pending) subscription version based on the active subscription version.

R5-35 SMS shall receive the following data from the usa to identify the active subscription version is to be modified: the Local Number Portability Service ID and the Ported Telephone Number Subscription ID.

R5-36 SMS shall allow the following data to be modified in the newly created subscription version:

Location Routing Number (LRN) - the identifier of the switches having portable NEs and used by the service providers <- at least one LRN is required.

LIDB GTT data - network addressing information for routing to serving LIDB.

DPC Type for LIDB features GTT - indicates whether Destination Point Code identifies the subsystem or a gateway.

GTT data for CLASS features - network addressing information for routing TCAP messages to the ported-to switch.

DPC type for CLASS features GTT - indicates whether Destination Point Code identifies the end office or a gateway STP.

R5-37 The following fields are for future use. The new facilitiesbased service provider may not be required to treat these fields as mandatory.

Billing Service Provider ID

End-User Location - Value

End-User Location - Type

Future 1

Future 2

Future 3

R5-38 SMS shall validate the modified subscription version. This validation process shall include the applicable validations deEmed in R5-18.

R5-39 If the version fails validation, S M S shall issue an appropriate error message to the request originator. A new subscription version shall not be created and no changes shall be made to the current active subscription version.

R5-40 If the version passes validation, S M S shall record the current date and time (i.e., system date and time) as the Activation Date and Time Stamp, shall mark the version with a status of sending in the SMS, and shall issue an appropriate message to the request originator indicating successful completion of the modify process.

R5-41 SMS shall activate the version in the network as defined in R5-51 through R5-61.

5.1.2.2.3 Conflict Subscription Version

An authorized NPAC user requests a subscription be placed in conflict or removed from conflict by associating an action of "conflict on" or "conflict off" with a version. This functionality is invoked when an authorized user requests that the version be placed in or removed from conflict.

5.1.2.2.3.1 Placing a Subscription Version in Conflict

R5-42 SMS shall receive the following data from the user to

identify the subscription version is to be placed in conflict: the Local Number Portability Service ID and the Ported Telephone Number Subscription ID.

R5-43 If the version status is not pending, SMS shall generate an error message and send it to the request originator. SMS shall not proceed further with the request to place the subscription version in conflict.

R5-44 If the version status is pending, SMS shall mark the version with a status of conflict. shall record the current date and time (i.e., system date and time) as the **Conflict** Date and Time Stamp and shall issue an appropriate message to the request originator indicating successful completion of the process to place a subscription in conflict.

R5-45 If a subscription version remains in conflict for thirty days, SMS shall invoke cancellation processing as defined in R571 (tuneable parameter). The user ID for this transaction shall be the "SMS System ID."

5.12.2.3.2 Removing a Subscription Version from Conflict

R5-46 SMS shall receive the following data from the user to identify the subscription version is to be removed from conflict: the Local Number Portability Service ID and the Ported Telephone Number Subscription ID.

R5-47 If the version status is not in conflict, SMS shall generate an error message and send it to the request originator. SMS shall not proceed further with the request to remove the subscription version from conflict.

R5-48 If the version status is conflict, SMS shall validate the subscription version. This validation process shall include the applicable validations defined in R5-18.

R5-49 If the version fails validation, SMS shall issue an appropriate error message to the request originator. A new subscription version shall not be created and SMS shall not proceed further with the request to remove the subscription version from conflict.

R5-50 If the version passes validations, SMS shall mark the version with a status of pending in the SMS and shall issue an appropriate message to the request originator indicating successful completion of the process to remove a subscription from conflict.

5.1.2.2.4 Subscription Version Activation

A user requests a subscription be activated in the network by associating a network action of "activate" with a version. This functionality, which can be invoked only by the new facilities-based service provida enables an authorized user to request that a subscription version be activated.

RS-S1 SMS shall receive the following data from the user to identify the subscription version is to be activated: the Local Number Portability Service ID and the Ported Telephone Number Subscription ID.

SMS shall record the current date and time (i.e., system date and time) as the Activation Date and Time Stamp.

R5-52 If the version status is not pending, SMS shall generate an error message and send it to the request originator.

R5-53 SMS shall re-validate the subscription version as per the validations defined in R5- 18.

R5-54 If the version fails re-validation, SMS shall log the error message(s) and make them available to authorized users, and mark the version status as invalid in the SMS.

R5-55 If the version is valid, SMS shall determine the Local SMS configuration data of all the Local SMSs.

R5-56 SMS shall translate the subscription version data to create interface messages containing the information to be updated to the Local SMSs.

R5-57 SMS shall send the interface messages to the Local SMSs. The subscription version shall be marked vith a status of sending in the SMS. SMS shall record the current date and time (i.e., system date and time) as the Broadcast Date and Time Stamp in the subscription version.

R5-58 SMS shall log the activation responses resulting from the activation requests sent to the Local SMSs. SMS shall allow users (with the appropriate security permissions) to view this information. The length of time that data will remain in this log shall be a parameter that is tuneable by the SMS Administrator.

R5-59 If a positive acknowledgment is received from all involved Local SMSs, then the subscription version shall be marked with a status of active in the SMS and the previously active version (if one exists) for the same subscription (i.e., ported TN) shall be marked as old.

R5-60 If the version fails activation in some of the Local SMSs to which it was sent (e.g., the link between SMS and a specific network node is down), the update shall remain in queue and shall be resent to the Local SMSs where activation failed. The number of automatic resends and the interval between resends shall be parameters that can be modified by the SMS Administrator. There shall be a default of three (3) for the number of retries and a default of two (2) minutes for the interval between resends. During this period, the status of the version shall remain "sending." Once the maximum queue time is exceeded, SMS shall consider the version to have failed activation at specific Local SMSs. SMS shall mark the status of the previously active vasion (if one exists) for the subscription (i.e., ported TN) as old. SMS shall send a notification to the NPAC System Administrator. This notification shall include the list of the

Local SMS(s) where activation failed. Special processing must be invoked by the NPAC System Administrator to resend the subscription version to the Local SMS(s) where it failed activation. The subscription version shall be marked with a status of failed and an indication that the failure was partial.

R5-61If the version fails activation in *all* the Local SMSs to which *it* was sent, SMS shall mark the status of the version as failed. If there is a current active subscription version, it shall remain active. SMS shall send a notification to the NPAC System Adrninistrator indicating that the subscription failed activation at all Local SMSs. Special processing must be invoked by the NPAC System Administrator to resend the subscription. The subscription version shall be marked with a status of failed.

5.1.2.2.5 Disconnect Subscription Version

When a user requests that an active subscription be disconnected, it will be deleted from the network. This functionality, which can be invoked only by the new facilities-based service provider, enables the usa to remove an active version from the network. The user-supplied Disconnect Date indicates when the customer's service was disconnected.

R5-62SMS shall receive the following data from the user to identify the subscription vasion is to be deleted: the Local Number Portability Service ID and the Ported Telephone Number Subscription ID.

R5-63If there is no subscription version with a status of active, SMS shall notify the request originator that the vasion is not active in the network and cannot be disconnected

R5-64If there is a subscription vasion with a status of pending, invalid, failed, or conflict and there is also a subscription vasion with a status of active, SMS shall notify the request originator that the active version cannot be disconnected until the pending, invalid, failed, or conflict vasion is canceled. SMS shall not proceed with the request.

R5-65 If the status of the current version for the subscription is active, SMS shall do the following:

translate the pending disconnect request to create an interface message identifying the subscription to be deleted by the Local SMSs,

send the disconnect message to the Local SMSs, and

mark the disconnect request with the status sending. SMS shall record the current date and time (i.e., system date and time) as the Broadcast Date and Time Stamp in the disconnect request.

R5-66 If the disconnect request succeeds in all the Local SMSs, SMS shall mark the current active subscription version with a status of old, shall update the Disconnect Date to the old subscription version, and shall mark the disconnect request as old.

R5-67 If the disconnect request fails in all of the Local SMSs, the status of the disconnect request shall be changed to failed. The current active subscription version shall remain active. SMS shall send a notification to the NPAC System Administrator that the disconnect request failed. Special processing must be invoked by the NPAC System Administrator to resend the disconnect request to the Local SMS(s).

R5-68 If the disconnect request fails in some of the Local SMSs to which it was sent (e.g., the link between SMS and a specific network node is down), the disconnect request shall remain in queue and shall be resent to the Local SMSs where the disconnect failed. The number of automatic resends and the interval between resends shall be parameters that can be modified by the SMS Administrator. There shall be a default of three (3) for the number of retries and a default of two (2) minutes for the interval between resends. During this period, the status of the disconnect request shall remain "sending." Once the maximum queue time is exceeded, SMS shall consider the disconnect request to have failed at specific Local SMSs. SMS shall send a notification to the NPAC System Administrator. This notification shall include the list of the Local SMS(s) where the disconnect request failed. Special processing must be invoked by the NPAC System Administrator to resend the disconnect request to the Local SMS(s) where it failed. The disconnect request shall be marked with a status of failed and an indication that the failure was partial.

5. 1.2.2.6 Subscription Version Cancellation

Only subscription versions with a status of pending, invalid, or conflict can be canceled. A user requests that a pending, invalid or conflict subscription be canceled in SMS by associating an action of "cancel" with a version. This functionality enables a user to cancel a subscription version that has not yet been activated in the network. Additionally, only NPAC personnel can cancel a subscription version with a status of conflict.

R5-69 SMS shall receive the following data from the user to identify the subscription version to be canceled:

the Local Number Portability Service ID and
the Ported Telephone Number Subscription ID.

R5-70 If there is no subscription version with a status of pending, invalid, or conflict, SMS shall issue an appropriate error to the request originator and shall not proceed with the request.

R5-7 1 If there is a subscription version with a status of pending, invalid, or conflict, SMS shall mark the subscription version with a status of canceled and record the current date and time (i.e., system date and time) as the **Cancellation** Date and Time Stamp.

5.1.3 Subscription Queries

The query functionality discussed in this section will give users the ability to view subscription data without being able to update that data. A user may not be able to modify a particular data item because that user does not have the proper security permissions and the data is made available via SMS for read-only purposes.

Assumptions

Users will need to be able to retrieve subscription data that they cannot modify.
Users shall submit query requests for subscription data based on a single ported TN only.
Any authorized service provider personnd shall be able to view any subscription version for any ported TN.

User Functionality

R5-72 An authorized SMS user shall be able to invoke the following functionality in the SMS to query subscription data:
Query data stewarded by SMS for a subscription and all its versions.

System Functionality

The following specifies SMS functionality needed to support the user requests defined above.
R5-73 For queries regarding subscription data, SMS shall receive the Local Number Portability Type [D and the Ported Telephone Number Subscription ID, and optionally, the status of the subscription version (e.g., active, pending).

R5-74

If multiple subscription vasions are found, and the user has provided the status of the subscription version desired, SMS shall retrieve only the data associated with that status of the subscription version only. Otherwise SMS shall return all subscription version data associated with the ported TN. The parameters to be returned, as appropriate for the subscription version status, are as follows: Local Nurnber Portability Type ID Ported Telephone Number(s) Due Date New facilities-based service provider ID Old facilities-based service provider ID

Authorization from old facilities-based service provider
Authorization from new facilities-based service provider
Location Routing Number (LRN)
LIDB GTT data
DPC type for L1DB features GTT
CLASS GTT data
DPC type for CLASS features GTT
Billing Service Provider ID
End-User Location Value
End User Location Type
Future 1
Future 2
Future 3
Disconnect Date
Conflict Date and Time Stamp
Activation Date and Time Stamp
Broadcast Date and Time Stamp

Cancellation Date and Time Stamp

R5-74 If SMS does not have a subscription version as specified by the request originator, SMS shall provide the request originator with a message indicating that there was no data in SMS that matched the search keys.

SECTION 6: NPAC SMS INTERFACES

Two interfaces to the NPAC SMS shall be supported. The first interface shall be between the NPAC SMS and the service provider's Service Order Activation platform and the second shall be between the NPAC SMS and the Local SMSs. Both of the interfaces shall support two-way communications.

6.1 SOA to NPAC SMS Interface

The SOA to NPAC SMS Interface could be used by a variety of local service provider systems for retrieving and updating subscription data in an NPAC SMS. The types of systems that are expected to use this interface are Service Provisioning OSs and/or Gateway Systems.

****
****

EXHIBIT

****
****

6.1.1 Request Administration

The SOA to NPAC Interface will support four types of transactions: subscription request and audit request transactions from the front end system (e.g., the SOA) interface users, and response and notification transactions from the NPAC SMS. The Interface will require security features to ensure that data is not corrupted by unauthorized access. Security management is outside the scope of the interface, however, the Interface user will be required to provide parameters to support security management at the NPAC SMS.

R6-1Associations on these application to application interfaces must use strong authentication.

R6-2Each subscription administration request sent over the Interface shall be capable of supporting multiple independent transactions. One failed item in a request will not cause other items in the request to fail. See ANSI standard T1.246, *Operations Adrninistration, Maintenance and Provisioning (OAM&P) -information Mode! and Services for Interfaces between Operations Systems across Jurisdictional Boundaries to Support Configuration Management - Customer Account Record*

Exchange (CARE) for an example of a GDMO (ISO 10165-4) description of an interface that can deal with bunched transactions.

R6-3 Each subscription administration request shall be acknowledged with at least one response transaction from the NPAC SMS. Some requests may be acknowledged more than once. For example, after validation processing is completed a response transaction would be sent back to the user with either a positive acknowledgment or a negative acknowledgment with an error message indicating the results of the validation.

6.1.2 Subscription Administration

Subscription Administration provides functionality in creating or modifying subscriptions and activating or deleting them from the networks. Based on security parameters, users of the interface shall be able to do the following:

R6-4 Add new versions of subscription data, as well as cancel or modify a specific version of subscription data.

R6-5 Retrieve subscription data, including either specific versions of a subscription or all versions.

R6-6 Request the activation or deletion of subscription data.

6.1.3 Audit Requests

Audit Request functionality enables users to obtain audits of a specific subscription or group of subscriptions at all service provider networks or at select networks. Based on security parameters, users of the interface shall be able to do the following:
R6-7 Request that an audit be performed for a subscription or a group of subscriptions.

R6-8 Specify that an audit be performed at all service provider networks or at select networks.

R6-9 Each audit request sent over the Interface shall be capable of specifying a single subscription or a range of TNs and specific search parameters.

R6- 10 Each audit request shall be acknowledged with at least one response transaction from the NPAC SMS. This response shall include an acknowledgment of whether discrepancies were reported by individual service providers and the identity of those providers. Audits which find no discrepancy shall receive one response. If discrepancies are found, there shall be one response per erred telephone number.

6. 1.4 Notifications

NPAC SMS shall have functionality to send notifications to service providers based on parameters which are tuneable by the NPAC SMS Administrator. NPAC SMS shall be able to do the following via the interface:

R6- 11 Notify a new or an old service provider that they haven't provided authorization for a transfer of service for a TN.

R6- 12 Notify an old service provider that the Due Date for a subscription has been modified

6.2 NPAC SMS to Local SMS Interface

The NPAC SMS to Local SMS Interface could be used to send subscription data and audit requests to a variety of service provider systems. The types of systems that is expected to use this interface are Local SMSs (or SMS-like functionality at LNP SCPs) and/or Gateway Systems. The interface will require security features to ensure that data is not corrupted by unauthorized access. Security management is covered in Section 7, however, the interface user will be required to provide parameters to support security management at the NPAC SMS.

****
****

EXHIBIT

****
****

6.2.1 Transaction Administration

The NPAC SMS to Local SMS Interface will support five types of transactions: subscription download transactions from the NPAC SMS, audit requests from the NPAC SMS, network data download transactions from the NPAC SMS, response transactions from the Local SMS, and requests from the Local SMS that specific transactions be resent.

R6- 13 Interface users shall specify their user-identification, system identification, and password to be able to use the Interface.

R6- 14 Each subscription download request sent over the interface shall be capable of supporting multiple independent transactions. One failed item in a request will not cause other items in the request to fail.

R6-15 Each subscription download request shall be acknowledged with at least one response transaction from the Local SMS. A response transaction shall be sent back to the NPAC SMS with either a positive acknowledgment or a negative acknowledgment which may include a request that the transaction be sent again.

R6- 16 Each audit request sent over the interface shall be for a single transaction or for a range of transactions.

R6-17 Each audit request shall be acknowledged with at least one response transaction from the Local SMS. A response transaction shall be sent back to the NPAC SMS with either a positive acknowledgment for those TNs which passed audit and a negative acknowledgment for those TNs which failed audit as well as only a negative acknowledgment for those TNs which failed audit.

R6- 18 A local SMS shall be able to request the NPAC SMS to resend a subscription based on its TN or a block of subscriptions based on a time window specified in the request. This function might be provided by allowing for an audit request from the local SMS.

R6-19Each network data download request shall be acknowledged with one response transaction from the Local SMS. A response transaction shall be sent back to the NPAC SMS with either a positive acknowledgment or a negative acknowledgment which may include a request that the transaction be sent again.

6.2.2 Network Subscription Administration

Network Subscription Administration provides functionality in activating, modifying, or deleting subscription data from the network and in requesting audits. The NPAC SMS, via its interface to Local SMSs shall be able to do the following:

R6-20 Add new subscription data, as well as delete or modify specific subscription data.

R6-21 Request audits of subscription data, including either a specific subscription or a range of subscriptions.

6.3 Interface Transactions

The CMIP protocol provides for seven types of transactions over the interface (Reference: ISO 9595 and 9596). They are Create, Delete, Set, Get, Cancel-Get, and Notification. The first six transactions are originated by the manager, and affect objects contained in the agent. The Notification transaction is created by the agent and is used to give notice *to* the manager that something of interest to the manager has happened to an object in the agent system.

R6-22 The object model shall be designed in terms of using these transactions in a manager-agent relationship.

6.4. Interface and Protocol Requirements

While it is expected that dedicated links will be used for the interfaces, switched connections should also be supported. Reliability and availability of the links will be essential and high capacity performance will be needed.

R6-23 The SOA to NPAC SMS Interface and the NPAC SMS to Local SMS Interface . shall be an open, non-proprietary interface.

6.4.1 Protocol Requirements

Both of the NPAC SMS interfaces, as defined above, shall be implemented via the following protocol stack:

R6-24:

Application: Presentation: Session: Transport: Network: Link:

Physical:

ASCE, CMISEEROSE (ANSI Tl.224) as described in ANSI Tl.224 as described in ANSI Tl.224 OSI Transport Class 0, RFC 1006, and TCP Internet (ETF) IP ethernet routing, or frame relay, or ATM (or more than one of these) as appropriate

R6-25 Multiple associations per service provider may be required.

6.4.2 Interface Performance Requirements

R6-26Both the SOA to NPAC SMS and the NPAC SMS to Local SMS shall be available on a 24 by 7 basis.

R6-27 A 99.9 % availability rate shall be maintained for both interfaces.

R6-28A transaction rate of 2 transactions per second shall be supported by each SOA to NPAC SMS interface association (See Section 10 for number of associations).

R6-29 A transaction rate of 25 transactions per second shall be supported by each NPAC SMS to Local SMS interface association (See Section 10 for number of
. .
assoclatlons.

6.4.3 Interface Performance Requirements

R6-30 The interoperable interface models shall be specified in terms of ISO 10165-4, "Generalized Definition of Managed Objects (GDMO)." The specification will become the property of the consortium, who may make it public.

R6-31 The model and interface specification shall be delivered in two stages.

R6-32 The model proposed shall be proposed shall be provided at the object and attribute level in the RFP proposal. It shall include tables and/or figures that show how the interface functions required by this specification were mapped into the services provided by the model.

R6-33The selected Prirnary vendor shall ddiver a complete interoperable interface specification one month after the announcement of the vendor selection.

R6-34 The application to application interfaces shall be specified in sufficient detail to allow the vendors who supply the SOA and Local SMS interfaces to build implementations that will interoperate with the NPAC SMS. This must be possible with no or only minimal interaction between the suppliers of the interoperable systems. For example the interoperable interface specification shall provide for error handling of error conditions appropriate to all of the functional requirements. It shall also define the security relationship between the systems.

R6-35 The interface specified shall be capable of extension to account for evolution of the interface requirements.

SECTION 7: SECURITY REQUIREMENTS

Introduction

In addition to the general security requirements based on the user interface paradigm in Section 7.1 through 7.7, there are requirements for the security on an OSI application to application interface (such as the one specified in Section 6 for the SMS to SMS and SMS to SOA interfaces). Section 7.8 describes such a security environment.

7.1 Identification

A user identification is a unique, auditable representation of the user's identity within the system. The SMS requires all system users, both individuals and remote machines, to be uniquely identified to support individual accountability.

R7-lUnique user identification codes (userids) must be utilized to identify individuals and remote machines.

R7-2SMS must require users, i.e., individuals and remote machines, to identify themselves with their assigned userid before performing any actions.

R7-3 SMS must maintain intemally the identity of all currently active users.
R7-4 Every process running on SMS must have associated with it the userid of the invoking user (or the userid associated with the invoking process).

R7-5 SMS must disable userids after a period of time during which the userid has not been used. The time must be NPAC-specifiable with a system delivered default of 60 days.

R7-6SMS must provide a complementary mechanism or procedure for the re-instatement or deletion of disabled userids.

R7-7SMS must support the temporary disabling of userids.

R7-8The mechanism that disables userids should provide an option for automatic reactivation.

R7-9SMS must control and limit simultaneous active usage of the same userids by allowing only one active login. When the second login is entered, the system will ask if the first login can be disconnected. If the user replies yes, the second login can continue; however, if the user replies no, the second login is terminated.

7.2 Autbentication

The identity of all system users, both individuals and remote machines, must be verified or authenticated to enter the system, and to access restricted data or transactions.

R7- 10 SMS must authenticate the identity of all system users, both individuals and remote machines, prior to their initially gaining access to SMS.

R7- l l SMS must not support ways to bypass the identity authentication mechanisms.

R7- 12 SMS must protect all internal storage of authentication data so that it cannot be accessed by
any unauthorized user.

7.2.1 Password Requirements

R7- 13 SMS shall not provide a mechanism whereby a single password entry can be shared by multiple userids.

R7-14 SMS must not prevent a user from choosing a password that is already associated with another userid.

R7-15 SMS must store passwords in a one-way encrypted form.

R7-16 Encrypted passwords must not be accessible to non-privileged users.

R7-17 Unencrypted passwords must not be accessible to any users, including NPAC personnel.

R7- 18 SMS must automatically suppress or fully blot out the clear-text representation of the password on the data entry device, e.g., terminal.

R7- 19 Passwords should not be sent over public or shared data networks in clear text.

R7-20 SMS must not allow for any password to be null.

R7-21 SMS must provide a mechanism to allow passwords to be user-changeable. This mechanism must require re-authentication of the user identity.

R7-22 The NPAC must have a mechanism to reset passwords.

R7-23 SMS must enforce password aging, i.e., passwords must be required to be changed after a NPAC-specifiable time. The system supplied default shall be 90 days.

R7-24 SMS must provide a mechanism to notify users in advance of requiring them to change their passwords. This can be done by one of the following methods: (1) SMS will notify users a NPAC-specifiable period of time prior to their password expiring. The system supplied default shall be seven days. (2) Upon password expiration, SMS will notify the user, but allow an NPACspecifiable subsequent number of additional logons prior to requiring a new password. The system supplied default shall be two additional logins.

R7-25 Password must not be reusable by the same individual for an NPAC-specifiable period of time. The system supplied default shall be six months.

R7-26 SMS must provide a method of ensuring the complexity of user-entered passwords that meets the following requirements:

(1) Passwords must contain a combination of at least six alphanumeric characters including at least one alphabetic and one numeric or punctuation character. If the system does not distinguish between upper and lower case alphabetic characters, the minimum acceptable length is eight characters.

(2) Passwords must not contain the associated userid.

R7-27 SMS-supplied password generation algorithms must meet the following requirements:

(1) Passwords must be "reasonably" resistant to brute-force password guessing attacks, i.e., the total number of system generated passwords must be on the same order of magnitude as what a user could generate using the rules specified in requirement 7-26 (1) above.

(2) The generated sequence of passwords must have the property of randomness, *i e* consecutive instances must be uncorrelated and the sequences must not display periodicity.

7.3 Access Control

Access to the SMS and other resources must be limited to those users that have been authorized for that specific access right.

7.3.1 System Access

R7-28 SMS must allow access to authorized users and authorized remote systems.

R7-29 SMS must provide a procedure for the initial entry or modification of authorized users and authentication information.

R7-30 SMS must not provide any default userids that can permit unauthenticated SMS access.

R7-31 SMS's login procedure should be able to be reliably initiated by the user, i.e., a trusted communications path should exist between SMS and the user during the login procedure.

R7-32 SMS must disconnect or re-authenticate users after an NPAC-specifiable period of non-use. The system supplied default shall be 60 minutes.

R7-33 The SMS login procedure must exit and end the session if the user authentication procedure is incorrectly performed an NPAC-specifiable number of times. The system supplied default shall be three times.

R7-34 SMS must provide a mechanism to immediately notify the NPAC when the above threshold is exceeded.

R7-35 When the above threshold has been exceeded, an NPAC-specifiable interval of time, not to exceed 60 seconds, must elapse before the login process can be restarted on that I/O port.

R7-36 SMS must not suspend the user id upon exceeding the above threshold.

R7-37 SMS must perform the entire user authentication procedure even if the userid that was entered was not valid.

R7-38 Error feedback must provide no other information except "invalid," i.e., it must not reveal which part of the authentication information is incorrect.

R7-39 SMS should provide a mechanism to exclude or include users based on timeofday, day-of-week, calendar date, etc.

R7-40 SMS should provide a mechanism to exclude or include users based on method or location of entry.
R7-41 SMS must provide a mechanism to limit the users authorized to access the system via dial-up facilities.
R7-42 SMS must provide a mechanism to limit system entry for privileged NPAC users on an NPAC-specifiable network access or per-port basis.

R7-43 Since some form of network access, e.g., dial-in, Wide Area Network, or Internet, is provided by SMS, SMS must provide a strong authentication mechanism. For example, the authentication mechanism could be a private or public key encryptionbased mechanism, an additional password, and/or smart card to validate the user or remote system. For remote machines, public key encryption may be required in conjunction with dedicated private lines. For dial-in users (NPAC administrative and NPAC operations), smart cards are required.

R7-44 A mechanism must exist to end the session through secure logoff procedures.

R7-45SMS must provide an advisory warning message upon system entry regarding unauthorized use, and the possible consequences of failure to meet those requirements.
R7-46 The message must be NPAC-specifiable to meet their own requirements, and any applicable laws.
R7-47 SMS must be able to display a message of up to 20 lines in length. This message should be displayed at the first point of entry. If possible, the message should appear before the logon process. As part of the delivered software, the following is an example of the default message that must be included:

NOTICE: This is a private computer system.
Unauthorized access or use may lead to prosecution.

R7-48 Upon successful access to the system, the following must be displayed:
(1) Date and time of the user's last successful system access.
(2) The number of unsuccessful attempts by that userid to access the system, since the last successful access by that userid.
R7-49 SMS must allow only the NPAC well-defined privileged users responsible for security administration to authorize or revoke users.
R7-50 Procedures for adding and deleting users must be well defined and described in the NPAC security documentation.

7.3.2 Resource Access
R7-51 Only authorized users shall be able to access the data that is part of or controlled by the SMS system.
R7-52 Each service provider's data must be protected from access by unauthorized users.

R7-53 Only authorized users shall be able to access the transactions, data, and software that constitute the SMS.
R7-54 The executable and loadable software must be access controlled for overwrite and update, as well as execution rights.
R7-55 Control of access to resources must be based on authenticated user identification.
R7-56 Encryption may be used to augment the access control mechanisms, but must not be used as a primary access control mechanism for sensitive data.
R7-57 For every resource controlled by SMS, it must be possible to grant access rights to a single user or a group of users.
R7-58 For every resource controlled by SMS, it must be possible to deny access rights to a single user or a group of users.
R7-59 It will be necessary to restrict user access to information based on the data content of a specific field, attribute, tuple, record, etc.
R7-60 Modification of the access rights to a resource must only be allowed by the NPAC.
R7-61 SMS must provide a mechanism to remove access rights to all resources for a user or a group of users.
R7-62 The access control mechanism's data files and tables must be protected from unauthorized access.

7.4 **Data and System Integrity**
R7-63 SMS must be able to identify the originator of any accessible system resources.
R7-64 SMS must be able to identify the originator of any information received across communication channels.
R7-65 SMS must provide mechanisms or procedures that can be used to periodically validate the
correct operation of the system These mechanisms or procedures should address:
(1) Monitoring of system resources
(2) Detection of error conditions that could propagate through the system
(3) Detection of communication errors above/below an NPAC-specifiable threshold
(4) Detection of Link Outages.
R7-66 SMS must be designed and developed to protect data integrity. This should include some
or all of the following:
(1) Proper rule checking on data update
(2) Proper handling of duplicate/multiple inputs
(3) Checking of return status
(4) Checking of inputs for reasonable values
(5) Proper serialization of update transactions
R7-67 NPAC documentation must contain recommendations for running database integrity
checking utilities on a regular basis.

7.5 Audit

7.5.1 Audit Log Generation

R7-68 SMS must generate an audit log that contains information sufficient for after-the-fact investigation of loss or impropriety and for appropriate response, including pursuit of legal remedies. The audit data shall be available on-line for a minimum of 90 days, and archived off-line for a minimum of two years.

R7-69 The user-identification associated with any SMS request or activity must be maintained, so that the initiating user can be traceable.

R7-70 SMS must protect the audit log from unauthorized access.

R7-7 1 Only well-defined privileged NPAC personnel can modify or delete any or all of the audit log.

R7-72 The audit control mechanisms must be protected from unauthorized access.

R7-73 SMS must cause a record to be written to the security audit log for at least each of the following events: (1) Invalid user authentication attempts (2) Logins and activities of NPAC users (3) Unauthorized data or transaction access attempts

R7-74 Auditing of NPAC actions must not be able to be disabled.

R7-75 For each recorded event, the audit record must contain, at a minimum: (1) Date and time of the event (2) User identification including associated terminal nort network srif4-v^^ ^communication device (3) Type of event (4) Name of resources accessed (5) Success or failure of the event

R7-76 Actual or attempted passwords must not be recorded in audit logs until after an NPAC-specifiable threshold of consecutive login failures. The SMS supplied default shall be three failures.

7.5.2 Reporting and Intrusion Detection

R7-77 SMS must provide post-collection audit analysis tools that can produce exception reports, summary reports, and detailed reports on specific data items, users, or communication failures.

R7-78 The NPAC must be able to independently and selectively review the actions of any one or more users, including other NPAC users, based on individual user identity.

R7-79 SMS must provide tools for the NPAC to monitor the activities of a specific network address or terminal in real time.

R7-80 SMS should contain a real-time mechanism that is able to monitor the occurrence or accumulation of security auditable events that may indicate an imminent security violation. This mechanism shall be able to notify the NPAC immediately when thresholds are exceeded, and if the occurrence or accumulation of these security relevant events continues, SMS shall take the least disruptive action to terminate the event.

7.6 Continuity of Service

R7-8 1 No service provider action, either deliberate or accidental, should cause the system to be unavailable to other users.

R7-82 SMS should detect and report conditions that would degrade service below a pre-specified minimum.

R7-83 Procedures or mechanisms must be provided to allow recovery after a system failure or other discontinuity without a protection compromise.

R7-84 Procedures shall be documented for software and data backup and restoration.

R7-85 The system must contain a database containing the exact revision number of the latest software installed.

Software Vendor

R7-86 The SMS software vendor must have a corporate policy governing its internal development of software. This policy must contain specific guidelines and requirements that are aimed at the security of its products, and are applicable throughout the software life cycle.

R7-87The SMS software vendor shall not design any mode of entry into the SMS for maintenance, support, or operations that would violate or bypass any security procedures.

R7-88The SMS software vendor shall not design any mode of entry into the SMS for maintenance, support, or operations that is not a documented feature of the SMS.

7.8 OSI Security Environment

This section examines potential threats to the NPAC SMS interfaces and proposes a set of security requirements to thwart such threats.

The security mechanisms described in the OSI Security segment are meant to illustrate the level of security and flexibility that is required for the OSI interfaces specified. The response to the RFP may propose different security mechanisms than the ones described. However, such security mechanisms should provide at least the same level of security and at least the same level of flexibility as the mechanisms described. The proposed mechanisms shall not be more difficult to manage, and should not require more processing or transmission capacity than the mechanisms described below.

7.8. 1 Threats

Attacks against the NPAC SMS may be perpetrated in order to achieve any of the following:

Denial of service to a customer by placing wrong translation information in the SMS

Denial of service to a customer by preventing a valid message from reaching the SMS

Disrupting a carrier's operations by having numerous spurious calls (to users who are not clients of that carrier) directed to that carrier

Switching customers to various carriers without their consent

Disrupting the functioning of the NPAC SMS by swamping it with spurious messages.

7.8.2 Security Services

The threats enumerated above can be thwarted by using the following security services:

R7-89 Authentication (at association setup)
R7-90 Data origin authentication for each incoming message
R7-91 Integrity - detection of replay, deletion or modification to a message
R7-92 Non-repudiation of origin

R7-93 Access control - allowing only authorized parties (i.e., carriers serving a given customer) to cause changes in the NPAC SMS database

7.8.3 Security Mechanisms

This section outlines the requirements for specific security mechanisms to support the security services enumerated above. For simplicity of presentation and without loss of generality, it assumes that information in the NPAC SMS is modified only in response to CMIP notifications from authorized entities.

7.8.3.1 Encryption

R7-94 Since non-repudiation must be supported a Public Key Crypto System (PKCS) must be used to provide digital signatures. Since there is no requirement for confidentiality service there is no need for any additional encryption algorithms. The NPAC SMS shall support one of the digital signature algorithms listed in the OIW Stable Implementation Agreement, Part 12, 1995.

R7-95 If a digital signature based on RSA encryption is chosen then the size of the modulus of each key shall be at least 600 bits. If another algorithm is chosen then the size of the key(s) shall be chosen to provide a level of security commensurate with RSA encryption with a 600-bits modulus.

R7-96 The digital signature algorithm shall be applied to ASCII representation of the signed data fields, without any separators between those fields or any other additional characters.

7.8.3.2 Authentication

R7-97 Strong, two-way peer authentication at association setup time shall be provided by using an authenticator (based on the authenticator used for the Trouble Administration application of Electronic Bonding as described in Committee T1 Technical Report No. 40 "Security Requirements for Electronic Bonding Between Two TMNs") consisting of

The unique identity of the sender

The Generalized Time corresponding to the issuance of the message, each party is responsible to assure that its system clock is accurate to within two minutes of GMT

A sequence number (equal to zero for association request and association response messages)

A key identifier

Any additional parameters required by the chosen digital signature algorithm, as specified in OIW Stable Implementation Agreement, Part 12, 1995

• The digital signature of the sender's identity, Generalized Time and sequence number listed above.

R7-98 The authenticator shall be conveyed in the CMIP access control field. (An appropriate syntax for this EXTERNAL field shall be provided.)

7.8.3.3 Data Origin Authentication

R7-101

R7-99 Every subsequent CMIP message that contains the access control field shall carry the authenticator described above in that field. Each party maintains a separate counter for the sequence number it uses. Every **time the** authenticator is used the value of the sequence number shall be incremented by one.

7.8.3.4 Integrity and Non-repudiation

R7-100 Because CMIP notifications do not have an access control field, all the notifications defined for the number portability application shall contain a security field. The syntax of the security field shall correspond to the authenticator defined above.

The values of the components of the authenticator shall also be as specified for the authenticator above, except that the digital signature shall apply to all the fields in the notification, except the security field, in the order in which they appear, followed by the GeneralizedTime and the sequence number. This ensures data origin authentication, integrity and non-repudiation of origin for each notification. In particular, the GeneralizedTime and the sequence number allow detection of deletion, replay and delay.

R7- 102 All the notifications shall be sent in the confirmed mode.

7.8.3.5 Access Control

R7-104The NPAC SMS shall be responsible for access control. In particular, it will assure that only authorized parties (current and future service providers for a given customer) can change information related to the number associated with that customer.

R7-105The only initiator-provided access control information that shall be used to this cffcst is thc authenticated ldenfity of the sender of the message that would result in a modification to the NPAC SMS database, and the value of the GeneralizedTime in that message (it should be within five minutes of the NPAC SMS system clock).

7.8.3.6 Audit Trail

R7-106The NPAC SMS shall keep a log (as defined in ISO/EC 10164 parts 6 and 8, 1992) of all incoming messages that result in the setup or termination of associations, all invalid messages (invalid signature, sequence number out of order, GeneralizedTime out of scope, senda not authorized for the implied request) as well as all incoming messages that may cause changes to the NPAC SMS database.

7.8.3.7 Key Exchange

R7-107There shall be an exchange of keys between the NPAC and each carrier it senses. DDg this exchange each party shall provide the other with a *list* of keys. The list shall be provided in electronic form. The originator of list of keys shall also provide the receiver with signed (in ink) paper copy of the MD5 hashes of the keys in the list. The lists can be exchanged in person or remotely. If the lists are exchanged remotely, they shall be conveyed via at least two different channels (e.g., a diskette sent via certified mail and file sent via e-mail).

R7-108Upon remote reception of a list of keys the recipient shall send an acknowledgment to the sender of the list. The acknowledgment shall consist of the MD5 hash of each one of the keys in the list. The acknowledgment shall be provided in electronic form via at least two different channels. In addition, the recipient shall call the sender by phone for further confirmation, and provide the sender with the MD5 hash of the whole list.

R7-109The NPAC shall issue periodically (e.g., once a month) a paper list of the MD5 hashes of all the public keys it uses and those of its clients. The list shall be sent to each client. Upon reception of the list and verification of its own the NPAC's public keys hashes, the client shall return an acknowledgment (by phone or mail) to the NPAC.

R7-110Each list shall consist of 1000 encryption keys, numbered from 1 to 1000, and 10 Key Encryption Keys (KEK), numbered from 1001 to 1010. Only encryption keys shall be used for digital signatures for normal number portability operations. They shall range in size (if RSA encryption is used) from 600 bits to 900 bits. (Larger keys shall be used in future years.) KEKs shall be used only to transmit a new list of keys, if necessary. The whole new list will be signed using a KEK. KEK sizes shall range from 1000 bits to 1200 bits (if RSA encryption is used). Keys in subsequent list shall be numbered from 2000 to 3010, 3000 to 4010, etc.

R7-111A new encryption key can be chosen with every message that contains a key identifier. After the usage of a key has stopped, that key shall not be used again. The key shall be changed every time there is a suspicion that the key has been compromised. The key shall be changed at least once a year. The keys used during a year shall be larger than the keys used the previous year by at least 20 bits.

SECTION 8: AUDIT ADMINISTRATION

Overview

An audit function will be necessary for troubleshooting a customer problem and also as a maintenance process to ensure data integrity across the entire LNP network. Audit will be concerned with the process of comparing the NPAC view of the LNP network with each service provider's network view. The service provider network may contain several network nodes designated for local number portability and may also choose to keep its own copy in its respective SMS. As a result, it will not be the responsibility of the NPAC to compare all network nodes but rather upon order of an audit request to have the service provider SMS report if a conflict exists in any of its designated LNP SCPs within its respective LNP network. The local SMS will compare the NPAC view of the data with the SCP view of the data.

Assumptions

SMS will contain the master copy of the data that it administers. Only the data administered over the NPAC SMS to Local SMS interface as a result of LNP subscription management will be audited.

8.1 Service Provider User Functionality

The following specifies the functionality required for audits issued by the service provider. These audit requests shall be issued from the service provider's SOA to the NPAC SMS. R8- 1 Service providers must be able to issue an audit request on a single telephone number. R8-2 Service providers must be able to issue an audit request for a range of telephone numbers. The size of the range of telephone numbers which can be specified must be a tuneable parameter set by the NPAC. R8-3 Service providers must be able to specify the scope of an audit by specifying one or more of the following parameters:
(a) Specific service provider network or ALL service provider networks.
(b) Full or partial audits, where the user can specify if one or ALL LNP attributes is to be audited, e.g., LRN, GTT or ALL. Default will be to audit ALL attributes.
(c) Indication whether to include non-ported numbers. For telephone numbers which fall within the range of telephone numbers specified and do not exist in the NPAC SMS database, then if this option is set these numbers will be audited, i.e., the NPAC SMS will ask the service provider's local SMS to return an indication if the record exists in its network or not. Default will be to not include non-ported telephone numbers.

8.2 NPAC User Functionality

Authorized NPAC personnel will have the capability to perform audits of the same nature as the service provider with some additional functionality. The NPAC SMS will provide a user interface for this purpose. This interface must support the following requirements of the audit function solely for execution by authorized NPAC personnel:

R8-4NPAC personnel will be able to issue an audit request on a single telephone number.

R8-5NPAC personnel will be able to issue an audit request for a range of telephone numbers. For the NPAC personnel there is no limit as to the size of the range specified.

R8-6The NPAC must provide the capability to issue an audit request to be executed immediately or a specific time in the future.

R8-7NPAC personnel will be able to specify if the audit request is to be periodic or a one time only request. Periodic audits can be specified to be issued weekly, monthly or quarterly. When a periodic type resumes execution, the audit will continue from where it last executed.

R8-8The NPAC user must be able to specify execution restrictions for an audit request. Execution restrictions include the following:
(a) Start time and end time window for the time period when the audit should execute.

R8-9The NPAC user must be able to specify the scope of an audit by defining one or more of the following parameters:
(a) Specific service provider network to be audited or ALL service provider networks.
(b) Full or partial audits, where the user can specify if one or ALL LNP attributes is to be audited, e.g., LRN, GTT or ALL. Default will be to audit ALL attributes.
(c) Indication whether to include non-ported numbers. For telephone numbers which fall within the range of telephone numbers specified and do not exist in the NPAC SMS, then if this option is set these numbers will be audited, i.e., the NPAC SMS will ask the service provider's local SMS to return an indication if the record exists in its network or not. Default will be to not include non-ported telephone numbers.
(d) Activation Date/Time stamp range, i.e., only audit records activated between a specific time window.
R8- 10 The NPAC user must be able to obtain the status of an audit request.
R8-11 The NPAC personnel must be able to obtain an audit's progress. Progress might indicate the percentage of records audited or the directory number of the record currently being audited assuming the records will be audited in a sequential fashion.
R8- 12 The NPAC personnel must be able to cancel an audit request.
R8-13 The NPAC personnel must be able to temporarily stop an audit which is currently in progress.
R8- 14 The NPAC personnel must be able to resume an audit which was temporarily stopped by the user or was stopped due to a failure which is now resolved.

8.3 System Functionality

R8- 15 All audit requests including requests issued by the service providers will be logged at the NPAC SMS and will be available for viewing by the NPAC personnel.

R8- 16 In order to execute the audit request, the NPAC shall send the audit request to the local service providers' networks via the NPAC SMS to Local SMS interface described in the LNP SMS Interface Specifications.

R8- 17 For all telephone numbers to be audited, the NPAC SMSwill send the telephone number record as it appears in the NPAC SMS to each service provider's local SMS. Upon receipt of the audit request, the local SMS will verify if the telephone number's entire record contents differs in its local network. The service provider's local SMSwiX verify the record contents in all respective SCP databases. The service provider's local SMSwill return an indication if any of its SCP databases is not in synch with the NPAC view of the data. For the case where non-ported numbers are being audited then the service provider's local SMSwiX report on the existence of the record in its LNP databases.

R8- 18 For periodic type audits, the audit will resume execution from where it last stopped after its previous execution.

R8- 19 The NPAC SMS must record all audit results in an audit log.

8.4 Audit Report Management

R8-20 Service Providers must be able to retrieve an audit report for a specific audit request via a specific transfer procedure offered for remote report retrieval as specified in the Reports management chapter.

R8-2 1 The NPAC SMS must generate an audit report for all audit requests. The audit report must indicate the following:

(a) Audit request parameters, e.g., Service Provider ID audited, telephone number range audited and other parameters which identified the scope of the audit.
(b) Date and Time of Audit.
(c) Progress key indication.
(d) Service Provider network which contains database conflict.
(e) A difference indicator which may indicate:
- mismatch between the NPAC SMS and local SMS
- record missing in local SMS
- record missing in NPAC SMS
- an audit failure
- no discrepancies found

R8-22 NPAC personnel must be able to generate and view an audit report.

R8-23 An audit report should be accessible while the audit is in progress so the current audit results can be viewed up to this point.

R8-24 The NPAC personnel must be able to output an audit report to a specified output device or to a text file.

R8-25 The NPAC personnel must be able to specify the length of time audit results will be retained in the audit log.

SECTION 9: REPORT MANAGEMENT

9.1 Overview

The NPAC SMS must support scheduled and ad hoc report generation for selectable reports. The report generation service shall create output report files according to specified format definitions, and distribute reports to output devices as requested.

A report distribution service is used to distribute report files to selected output devices.

Authorized NPAC personnel can request reports from active database, History Logs, Error Logs, traffic measurements, usage measurements, and performance reports.

Examples of the items available from active database are:

- List of ported TNs for a service provider
- List of pending subscription orders for a service provider
- Subscriptions without concurrence - Status of pending subscription order for a TN being ported
- Date/Time Stamp of Subscription Port (Activation)
- Date/Time Stamp of Subscription Disconnect (Activation)
- Records that required conflict resolution Previous service providers and dates of service for ported TNs
- Date/Time Stamp of Broadcast time for transactions
- Subscription order records in error
- Download requests in error
- Log of Missing Response from SOA for order matching
- Log of Missing Response from Local SMS for downloads
- Log of Unauthorized Access Attempts
- Counts of events and usage as described in resource accounting.

Performance Reports

- CPU usage.

- Number of transactions handled and transactions per second.

- Measure of time starting from the receipt of subscription order activation to the broadcast of transaction to Local SMSs.

- Measure of time starting from the receipt of subscription order activation to the receipt of response from Local SMSs.

- NPAC SMS to Local SMS link utilization

- NPAC SMS to SOA link utilization

9.2 User Functionality

R9-1 The NPAC personnel must be able to select the type of report required.

R9-2The NPAC personnel must be able to select the output device destination (printer or other destination) for the report.

R9-3The NPAC personnel must be able to save/reprint reports from backed up output files.

R9-4The NPAC personnel must be able to create customized reports through an ad-hoc facility.

R9-5The NPAC personnel must be able to define scope and filtering for items to be included in the customized reports.

R9-6The service provider users must be able to receive reports on information related to their activities.

R9-7 Vendors must provide examples of report outputs.

9.3 System Functionality

R9-8The NPAC SMS must provide easy to read on-line and hard copy reports of the requested information.

R9-9The NPAC SMS must verify whether the user requesting the report has the proper viewing privileges for the selected data.

R9-10 The NPAC SMS must support on-line file transfer capabilities (e.g., FTP or FTAM) to transfer report files.

R9- 11 The NPAC SMS must maintain a History Log to keep track of transaction processed.

R9- 12 The NPAC SMS must maintain an Error Log to keep track of transaction errors, transmission errors, unauthorized access attempts.

R9-13 Vendors must specify a list of available output device options.

SECTION 10: NPAC SMS RELIABILITY, AVAILABILITY, PERFORMANCE AND CAPACITY

This section defines the reliability, availability, performance and capacity requirements for the NPAC SMS.

10.1 Availability and Reliability

The NPAC SMS will be designed for high reliability, including fault tolerance and data integrity features, symmetrical multi-processing capability, and allow for economical and efficient system expansion. The system will adhere to the following availability and reliability requirements:

R10-1 It wiU be available 24 hours a day, 7 days a week.

R10-2 It's reliability win be 99.9%. This applies to an functionality and data integrity.

R10-3 The amount of unscheduled downtime per year will be <= 9 hours.

R10-4 For unscheduled downtime, the mean time to repair will be <= 1 hour.

R10-5 The amount of scheduled downtime per year will be <= 24 hours.

R10-6 It win be capable of monitoring the status of all of its communication links and be capable
of detecting and reporting link failures.

R10-7 It win be capable of detecting and correcting single bit errors during data transmission
between hardware components (both internal and external).

R10-8 If a failure occurs resulting in downtime of any functionality, affected transactions received
immediately prior to the failure must be queued and processed when functionality resumes.

R10-9 The design will provide:

- Functional components with on board automatic self checking logic for immediate fault locating.

- Continuous hardware checking without any performance penalty or service degradation.

- Duplexing of all major hardware components for continuous operation in the event of a system hardware failure.

- Hardware fault tolerance that is transparent to the service providers.

R10-10 If the system becomes unavailable for normal operations due to any reason, including both scheduled and unscheduled maintenance, service providers must be notified of the system unavailability.

- When possible, the notification will be made via an electronic broadcast message to the service providers. When this is not possible, the NPAC will notify the service providers via their contact numbers.

- The notification will include, at a minimum, the functionality that is unavailable, the reason for the downtime, estimated length of the downtime and a NPAC contact number.

R10- 11 Dunng any maintenance, if resources allow only partial functionality, the capability of receiving, processing and broadcasting updates will be given the highest priority.

R10- 12 It must provide system tolerance to communication link outages and offer alternate routing during such outages.

R10-13 For any downtime, either schedule or unscheduled, lasting more than 1 hour, the NPAC SMS will switch service providers to a backup or disaster recovery machine as described in section 2. In most cases, the time to switch the service providers to another machine and provide full functionality must not exceed the mean time to repair . However, in the event of a disaster that limits both the NPAC and NPAC SMS ability to function:

- The capability of receiving, processing and broadcasting updates must be restored within 24 hours.

- Full functionality must be restored within 48 hours.

The vendor is requested to describe the architecture used to satisfy the reliability and availability requirements, including any the use, if any, of a backup and/or disaster recovery machine and the use of any disaster recovery location. Alternatives to the backup and disaster recovery process flow in section 2 should be included here.

R10- 14 Reports documenting the performance of the NPAC SMS in regards to the above requirements will be provided periodically to the service providers.

10.2 Capacity and Performance

The following requirements define the capacity and performance of the NPAC SMS. While the initial transaction rates and data storage requirements are not high, the NPAC SMS is expected to provide high performance and allow for future expansion. Refer to section 13 for future expansion possibilities.

R10-15 The system will be engineered to allow for 30 service providers having SOA and SMS interfaces. On initial turnup, it is expected there will be 10 service providers having SOA and SMS interfaces.

R10- 16 Describe any capacity requirements related to the NPAC personnel who will be users of the NPAC SMS.

R10- 17 It will be capable of handling the following transaction rates. Each record added or updated involves 1 transaction from the old service provider, 2 transactions from the new service provider and a broadcast to every service provider. Transaction rates are projected in three categories, i.e., High, Medium, and Low:

	HIGH	MEDIUM	LOW
Year 1:	70,000	50,000	25,000
Year 2:	100,000	70,000	50,000
Year 3:	500,000	250,000	100,000
Year 4:	750,000	500,000	250,000
Year 5:	1,000,000	500,000	500,000

The number of updates due to mass changes, the number of audit requests and the number of report requests is not known at this time.

R10-18 Data storage of the History file must keep track of all transactions made for one year (churn and new records.) It is assumed that there will be thirty percent churn of accumulated records.

R10- 19 From the time an activation notice is received from the new service provider to broadcast out an update until the time the update is broadcasted to all service providers will be < 60 seconds.

R10-20 The response time from when a request or transaction is received in the system to the time an acknowledgment is sent to will be < 3 seconds. This does not include the transmission time across the interface to the service provider's SOA or SMS.

R10-21 The NPAC SMS must be expandable to handle any future growth due to circumstances described in section 13.

1 1.1 Overview

Resource Accounting allows the tracking of NPAC resource usage data, which may be used as a basis for billing the service providers for their use of NPAC functionality. Resource Accounting is responsible for gathering the information into usage measurement categories, aggregating the measurements, and formatting and outputting the measurements to the appropriate entities (e.g., Billing Operations Applications, service providers). Other potential applications for usage information include cost allocation, marketing, and usage studies.

The NPAC system cost recovery methods should be designed to recover initial system costs, as well as the on-going operations/maintenance/administration costs. The vendors shall describe the cost drivers for NPAC HW/SW platform, including a breakdown of cost for the major features. The vendors may propose additionaUalternate measurements that are based on their specific implementation, and provide measure of usage of the relevant cost causing elements in the NPAC system. The vendors shall describe their proposals for cost recovery and billing to the participating service providers.

The following are some examples of items measured for each service provider:
A. Duration of login session, date/time, service provider ID, user login ID, of login session
B. Number of transactions (port/ disconnect/cancel) processed
C. Counts of types of updates made (e.g., # of port, # of disconnect)
D. Number of errors encountered in transactions
E. Number of errors encountered during transmission
F. Number of current records maintained
G. Number of pending records maintained
H. Number of history records maintained
I. Number of records downloaded as normal action
J. Number of records sent in response to a resend request
K. Number of records re-sent due to transmission problems
L. Number of records in conflict
M. Number of missing responses (e.g., during order matching)
N. Number of records audited on request
O. Number of records corrected (e.g., as result of audit)
P. Number of records queried/ viewed
Q. Amount of data transported to Local SMS as bulk load update
R. CPU usage

S. Failures and maintenance problems in the NPAC SMS

Please indicate what other measurements may be made.

1 1.2 Assumptions

The service providers will be billed in proportion to their usage of the NPAC system services.
The resource accounting measurements will not cause degradation in the performance of the basic
functions of the NPAC.

1 1.3 User Functionality

R 11 - 1 The NPAC personnel shall be able to turn on or off the generation of usage measurements for each of the usage types.

1 1.4 System Functionality

R11-2 The NPAC SMS shall measure and record the usage of NPAC resources on a per service provider basis to cost allocation / billing.

R11-3 The NPAC SMS shall generate usage measurements for login sessions, for each service provider SP.

R11-4 The NPAC SMS shall generate usage measurements for the allocated mass storage (number of records stored), for each service provider.

R11-5 The NPAC SMS shall measure the number of transactions processed, for each service provider.

R11-6 The NPAC SMS shall measure the number of transactions downloaded to each service provider.

R11-7 The NPAC SMS shall measure the number of records sent in response to a request for resend of data from the service provider.

R11-8 NPAC should be able to render detailed periodic bills to the contracting entity.

SECTION 12: NUMBER PORTABILITY ADMINISTRATION CENTER

12.1 **Number Portability Administration Center (NPAC)**

NPAC Role

The NPAC will be staffed by a neutral third party contractor who will be responsible for the administration and operational support services required by service providers in their use of the NPAC SMS. The NPAC must be run in support of consortium of local service providers. As a result of agreed-to guidelines, the NPAC will be involved in local ported number administration monitoring. Mechanized enforcement capabilities may or may not exist in the NPAC SMS to assist the NPAC in the monitoring and control functions.

Operational Functions

The primary roles of the NPAC are to assist users in obtaining reliable access to the NPAC SMS and to support all users encountering local ported number service provisioning problems resulting from NPAC SMS operation. To meet this need, the NPAC must support the following functional areas: System Administration, User Support, and System Support.

Administrative Functions

Administrative functions include all management tasks required to run the NPAC. The NPAC Contractor must be accountable for all personnel, legal, and financial management associated with the NPAC. These include, but are not limited to billing management, staffing, equipment and site procurement, facilities, and the contractor's own accounts payable obligations, which are part of day to day management. The NPAC contractor must provide for the administration of its staffing, contractual, financial, and operational needs. Proposals must specify how this will be accomplished.

The NPAC will be responsible for working with Local service providers to update data tables required to route calls for ported local numbers. The NPAC is also responsible for distributing the most current version of ported local number administration guidelines.

NPAC staff performing these activities needs to combine strong project planning skills, organizational management experience, interpersonal communication and negotiation skills, and a clear understanding of the day-to-day business issues associated with running a successful NPAC. The NPAC manager and administrative staff ideally would come from a data processing environment requiring these attributes.

System Administration

System administration is the NPAC operational group responsible for NPAC SMS logon administration, user access and customer data security, user notification of scheduled system downtime, and management and administration of the NPAC SMS information tables required to link customer records with the correct ported number service functions, features, and network routing information.

1 2.2 Logon Administration

Key Responsibilities

- Assist with new logon requests
- Verify logon signature approval
- Initialize logon ID, password, and security level
- Update data base and add new users
- Notify user cxf logon activation
- Resolve problems with existing logon IDs or passwords

Procedure Description

Logon Administration provides an individual requiring access to the NPAC SMS system with a unique logon ID and password upon receipt of an approved request form.

Access is initiated upon receipt of a completed NPAC SMS logon ID request form having the proper signature approvals from the requesting organization and the NPAC manager. Afta access approval, the logon administrator will assign the logon ID and appropriate security level corresponding to the type of NPAC SMS user. The user's security clearance sets the correct level of customer record access and NPAC SMS functional capabilities. After the logon is initialized and entered into the NPAC SMS, the users are informed of the logon activation, and a completed NPAC SMS logon ID request form is mailed back to them for their records.

Logon administration is responsible for resolution of any of the user's NPAC SMS access problems that the User Support group cannot solve. All problems should be recorded as NPAC consultation reports and entered as trouble reports into a mutually agreed upon trouble reporting system. The NPAC must attempt to resolve all problems in real-time. Those requiring additional assistance will be assigned a priority level in the trouble report system and the appropriate NPAC SMS support group will be contacted directly. The NPAC is required to report issue resolution status back to the reporting party on a timely basis.

12.3 Customer Record Security

Key Responsibilities

- Establish user boundaries through user access permission classes
- Assign new users to the correct security permission class
- Exercise absolute control of access to customer records
- Monitor and report unauthorized system access attempts

Procedure Description

Closely linked with logon administration is the procedure that provides the correct level of system access and customer data record access. The permitted level of access depends on the classification of NPAC SMS user. Before any logons are assigned, a security group will be associated with a specific classification of NPAC SMS user. The NPAC

will establish boundaries for the appropriate level of customer record access and feature set functionality.

When the security groups are configured, any logon request that is received must be assigned to the correct user class. The logon Administrator is responsible for determining the correct group based on the organization that originates the request.

1 2.4 Scheduled System Unavailability Notification

Key Responsibilities

Notify users in advance of planned or known system unavailability

Procedure Description

In concert with the System Support group, System Administration is responsible for notifying NPAC SMS users of scheduled periods of system shutdown. These periods may be due to routine maintenance of the system or the result of non-critical system failures that require a brief and immediate shutdown of the system for repairs. Users are given sufficient warning to complete their current transactions and exit the system without loss of information. Users will usually be made aware of periods of system shutdown via electronic mail capabilities of the NPAC SMS.

12.5 Software Release Acceptance Testing

Key Responsibilities
- Update software test plans
- Allocate staff for performing tests
- Execute test plans
- Generate and resolve testing trouble reports
- Document test results
- Certify NPAC SMS software and release for operation

Procedure Description

The NPAC is required to perform acceptance tests on every release of the NPAC SMS system software before certifying it for operational release. The NPAC SMS release test plan must be reviewed and updated by the NPAC contractor for each NPAC SMS release, including testing of new features or existing features that have been modified and any major fixes that have been implemented. It is the responsibility of the NPAC contractor, as part of an acceptance test plan to fully regression test major releases.

The System Adrninistration group is responsible for testing those functions associated with its specific procedural duties included in the NPAC release test plan. These include, but are not limited to the following:

System Logon and Security Features
NPAC SMS administrative data table update features
Customer record features
Electronic mailbox features

Completion of acceptance tests will result in a release certification report summarizing all the test results, including those errors encountered and the resolutions required to successfully pass the tests.

1 2.6 Service Administration

Key Responsibilities

- Create and maintain NPAC SMS data table
- Map table information to appropriate codes (e.g., NPA, LRN, GTT)
- Create and maintain descriptive data table labels

Procedure Description

The Tables Administration function within the System Administration group is responsible for creating and maintaining internal NPAC SMS data tables used to validate data entries and minimize user input errors through the use of appropriate quality assurance and quality control methods. There are several different types of tables which can be grouped into mapping, validation, and NPA splits/mass changes tables, which include, but are not limited to the following:

- Location Routing Number (LRN) tables
- Service Provider GTT information tables
- RAO codes
- Service Provider codes

The procedures associated with table administration vary depending on the table involved.

12.7 Mass Change Administration

Key Responsibilities Maintain a close working relationship with organizations responsible for NPA split/mass changes scheduling.
- Analyze split or mass change impact on NPAC SMS administrative tables
- Analyze split or mass change impact on NPAC SMS customer records
- Notify pending split to appropriate service provider service administration centers.
- Coordinate with data center vendor to execute NPAC SMS programs required to perform table and record modifications.

Procedure Description

The splitting of an NPA and the resulting mass changes required to NPAC SMS records are elements of an infrequent and complex process beginning more than one year before the cutover date. The NPAC becomes involved after receiving notification from the company responsible for the split. The goal of the NPAC is to transparently transition affected records in the NPAC SMS data base to reflect the new NPA information.

The first step in the process is to analyze the impact of the split on the NPAC SMS table and record information. After impact analysis and record sorting have been completed the NPAC will work closely with the NPAC SMS data center support group to include the modifications as part of the data base.

Specific tasks performed by the group are routine and procedural. Staff members will need to have clerical data processing skills and training in on-line computer processing. Types of problems resolved by the System Administration Staff will primarily concern user access and system security issues. Procedures are needed for mass changes other than NPA splits such as LRN or DPC changes.

User Support Group

The User Support Group is the primary NPAC contact for NPAC SMS users encountering problems with system features, or with inputting or accessing of their customer record data. The group would also be responsible for the dissemination of NPAC SMS status information, such as scheduled downtime, new software releases, documentation updates, and training registration information.

This group provides the NPAC SMS user a central point of contact for resolution of NPAC SMS problems and trouble reporting. Resolution of user problems will be handled primarily through the efforts of the User Support Group itself. Those issues requiring the efforts of another NPAC group will be promptly referred to the appropriate group. Issues requiring Vendor or NPAC SMS Data Center operations support must always be researched first by the responsible NPAC staff member The key point of contact for users will always reside within the NPAC for NPAC SMS service Issues.

1 2.8 User Problem Resolution

Key Responsibilities

- Resolve customer record access problems
- Clarify feature capabilities for users
- Resolve customer record input and modification problems
- Perform acceptance testing for new software releases
- Support link problem resolution with datalink protocol analysis capabilities

Procedure Description

The primary function of the User Support Group is solving the problems of the NPAC SMS user. Phone calls to the User Support Group must be dealt with as they are received, with the goal of real-time problem resolution (i.e., within one hour). If this requires the assistance of another group within the NPAC, the call should be transferred to a staff member who can better aid in resolving the issue. This requires the User Support staff to be knowledgeable in all NPAC regpongibilitieg and aware of specific expertise The PAC is responsible for responding to the user with either an answer or a date by which an answer will be available. If the problem is determined to be critical it will be given priority within the NPAC.

1 2.9 Software Release Acceptance Testing

Key Responsibilities

- Update software test plans
- Allocate staff for performing tests
- Execute test plans
- Generate and resolve testing trouble reports
- Document test results
- Certify NPAC SMS software and release for operation

Procedure Description

The NPAC is required to perform acceptance test on every release of the NPAC SMS system software before certifying it for operational release. The NPAC SMS release test plan must be reviewed and updated by the NPAC contractor for each NGAC SMS release including testing of new features or existing features that have been modified. It is the responsibility of the NPAC contractor to fully regression test major releases.

The User Support group must work with the administrative organization to test those functions associated with its specific procedural duties included in the NPAC release test plan which include but are not limited to:

- Customer record features
- Electronic mailbox features
- Help messages

Resolution of testing problems must occur to complete testing and gain approval of the software release. Completion of the acceptance tests will result in a release certification report summarizing
all the test results, including those errors encountered and the resolutions required to successfully pass the tests.

12.10 Software Update Notification

Key Responsibilities

- Notify users of upcoming NPAC SMS software releases

Procedure Description

In an administrative capacity, the User Support Group is responsible for keeping the NPAC SMS user community abreast of system software update activity. The notifications must include the specific reasons for the new release and summaries of what is being added, deleted, or modified with respect to system features and capabilities. If the release was unscheduled and is the result of resolution of several critical system problems, the notifications must summarize all problems being corrected. Updated documentation should be included as part of the software update.

12.11 Training Administration

Key Responsibilities

- Serve as primary contaa for course schedules/registration information
- Ensure availability of all NPAC SMS training

Procedure Description

The User Support Group is responsible for managing the availability of NPAC SMS training courses and the handling of user registration requests. The NPAC may develop and administer all NPAC SMS training independently, or procure from another qualified training vendor, the facilities and instructors necessary to teach the courses. The training materials must be procured

from a qualified vendor. The NPAC will also perform training registration. Course schedules will be negotiated between the User Support Group and the training vendor, based on course demand forecast by the User Support Group. The training vendor will be responsible for billing attendees directly.

12.12 Document Order Administration

Key Responsibilities

- Process documentation requests
- Provide billing documentation
- Initiate documentation update distribution
- Provide documentation description, ordering information and price list literature

Procedure Description

In an administrative capacity, the User Support Group is responsible for handling user requests for NPAC SMS documentation. The NPAC will maintain an inventory of available NPAC SMS documentation for quick processing of orders, as available. The NPAC will handle all customer billing for documentation. Phone in documentation inquiries should be handled immediately. If documentation description, pricing, or ordering information literature is requested, it must be mailed to requester within 24 hours. Orders should be accepted only from companies with active system logons and must be accompanied by a documentation request form. Facsimiles should be accepted in emergency situations. Documentation billing will be added to the NPAC SMS user's service bill.

12.13 Training and Documentation User Feedback

Key Responsibilities

- Getting appropriate user recommendations reflected in NPAC SMS system documentation and training material

Procedure Description

User feedback for NPAC SMS training and documentation is just as important as feedback receiver for the operational system itself. The User Support Group is responsible for recording the feedback received during phone in conversations. Those comments pertaining to training and documentation must be recorded and entered into the trouble reporting system just as a service problem would be entered. Analysis of the impact of a problem on training or documentation material should be included as part of the impact analysis done for every trouble report entered into the trouble system.

12.14 SCP Download Problem Resolution

Key Responsibilities

- Analyze and resolve exception report issues resulting from unsuccessful updates to Local service providers' networks

Procedure Description

Failures in the download of customer records to the service providers Networks served by NPAC SMS are reported to the NPAC User Support Group. User Support staff must resolve all download failures.

Failures will primarily be the result of unsuccessful sending of customer records and/or NPAC SMS administrative instructions to the receiving service provider network. Resolution of customer record download failures to an service providers network must have the highest priority. Resolution efforts must continue until the problem is solved, with the service provider receiving notification when the updates are successfully completed.

The User Support Group requires staff who are well versed in all NPAC SMS capabilities. The ability to learn from many different user problems and to quickly relate a given problem to a previous experience will ensure successful user support. The User Support staff must also speak English clearly. have excellent communication skills to effectively interact with NPAC SMS users and take prompt action to resolve problems.

System Support Group

The System Support group is responsible for resolving or coordinating resolution of all user or NPAC SMS problems relating to system availability or technical communication problems. This group will be responsible for maintaining reliable system communication linkages between NPAC SMS and all other local number systems that rely on NPAC SMS for information updates. These will include, but are not limited to service providers' networks used *to* perform call routing functions, Directory Assistance Provider's system (when available), local exchange carrier Revenue Accounting Offices, Signaling and Engineering Administration Centers (SEAC or equivalent organizations) and other NPAC SMSs. The NPAC SMS will generate a multitude of system performance, customer record, and problem exception reports. The System Support group must be able to interpret, generate, and distribute reports requested by an NPAC SMS user.

12.15 NPAC SMS Report Administration

Key Responsibilities

- Generate and distribute NPAC SMS reports to all requesting users who are entitled to receive reports

- Validate the accuracy of report contents

- Generate and distribute reports to NPAC SMS users who are entitled to receive reports and do not have local print facilities

- Resolve report interpretation problems

Procedure Description

The System Support group is the key point of contact for resolution of problems pertaining to NPAC SMS reports. The System Support group must ensure that the system is able to produce requested reports and assist in the validation and interpretation of any report. As with other NPAC SMS problems the System Support staff will file a trouble report in the system for evaluation and record keeping. Any NPAC SMS user with an active NPAC SMS logon can view or obtain copies of those reports allowed by the security associated with their logon ID.

12.16 Failure Recovery Administration and User Notification

Key Responsibilities

- Notify all NPAC SMS user groups of an unscheduled system shutdown or failure

- Serve as the key point of contact for system recovery status

Procedure Description

In the event of an unscheduled, instantaneous system shutdown or failure, the NPAC SMS Data Center operations staff will notify the NPAC System Support group within five minutes of failure. Within 15 minutes of failure, the NPAC will notify the NPAC SMS user community. Notification will be through an NPAC SMS broadcast message. If the system is not available the NPAC must provide a system status hotline number that users can call to obtain the latest system information. The NPAC will receive updated system status from the NPAC SMS data center at agreed upon intervals, and convey that information to the users via the NPAC SMS system or hotline. The NPAC will inform the NPAC SMS users of the data base status after the problem is fixed. Users will need to know the time period during which transactions were lost and affect restoration to the best of their abilities, while the NPAC will help in reconciliation.

12.17 NPAC SMS Interface Monitoring

Key Responsibilities

- Assist in the resolution of data communication problems with other NPAC SMS service systems (service providers, Operator Service Systems, RAOs, etc.)

- Provide technical assistance to NPAC SMS users experiencing problems accessing the system

- Generate automatic audit reports

Procedure Description

The objective of this System Support function is to provide reliable NPAC SMS user access and system communication with other ported nusnber service system components through the performance of routing functional audits. These audits must be organized into a suite of tests that are run periodically, and at least every week. The results of these audits will be used by more technically trained staff to detect potential system performance or availability problems. In all cases the System Support group must be responsible for coordinating the resolution of issues involving user access to the NPAC SMS. NPAC SMS problems will typically be referred to System Support through phone calls received by the NPAC User Support group. All issues must be documented in the form of a NPAC consultation report, and, if due to a system failure, must be recorded as a trouble report in the trouble reporting system.

12.18 Software Release Acceptance Training

Key Responsibilities

- Update software test plans
- Allocate staff for performing tests
- Execute test plans
- Generate and resolve testing trouble reports
- Document test results

- Certify NPAC SMS software and release for operation

Procedure Description The System Support group is responsible for testing those functions associated with its specific procedural duties included in the NPAC release test plan. These include, but are not limited to:

- NPAC SMS report availability verification
- NPAC SMS service maintenance and diagnostic procedures
- NPAC SMS-Service Provider administrative functions

Resolution of testing problems must occur to complete testing and gain approval of the software release. The NPAC will work with the platform provider to resolve NPAC SMS system related problems. All problems will be recorded in the trouble reporting system. Key attributes staff members of the System Support group must possess the ability to diagnose a problem using a strong set of technical system skills, and quickly disseminate that information to the appropriate NPAC or Vendor Support groups to rectify the situation. Personnel staffing these positions need to have strong data processing, problem diagnosis and system communication skills and previous experience supporting a data processing operation. Specific skills include knowledge of the NPAC SMS System Vendor's Information Management System for data base systems, operating system, and their wide area data communications protocols.

NPAC Organizational Interface Requirements

In meeting contractual requirements the NPAC contractor will be required to interact with a diverse set of organizations, especially the full range of NPAC users. The most common user will be companies using the NPAC SMS as the centralized data base for their provisioning of ported local numbers for their customers. The NPAC will also work with the service providers' support and service administration organizations which use ported local number routing instructions. The NPAC must be able to work with service providers utilizing multiple software vendors. All users will identity their primary contacts to the NPAC for each area

NPAC SMS Data Center

The NPAC contractor will also manage the data center operation and as such, they shall be required to provide hardware, operational support for NPAC SMS application(s) including systems engineering to integrate computer system and communications components. The NPAC SMS data center is redundant. (Further Reliability requirements are outlined in Section 10.)

The NPAC contractor will have direct contact with the data center operations staff to assist in resolution of NPAC SMS access and communication problems. Coordination of scheduling and execution of special NPAC SMS table administration, NPA splits, and mass change programs will be handled by the NPAC with the data center operation. The NPAC and the data center will share information necessary to plan for growth or reconfiguration of the hardware platform and communications.

12.19 Administration

The administrative staff must provide support and direction for the operational NPAC groups and manage the business and technical issues affecting the performance of NPAC services.

Key Responsibilities

- Plan NPAC staff for software acceptance testing, report acceptance results, and ensure problem resolution of discrepancies.
- Schedule staff training for new software features and updates Analyze documentation and training impact
- Coordinate testing and cutover with NPAC SMS data center operations
- Coordinate critical software release cutover
- Provide billing for service providers' usage
- Manage NPAC accounts receivable collection
- Manage NPAC accounts payable responsibilities
- Resolve any NPAC billing disputes
- Process bills to NPAC from data center operations and system vendor for support services
- Adjust Staffing Level Based on Forecast System Usage Demands
- Plan capital equipment based on required staffing levels and NPAC performance standards
- Manage NPAC facilities
- Monthly status reports on total billing, summary of customer service activities, transactions, and trouble reports, summary of administrative and other support activities
- List of trouble reports, with a breakdown between NPAC SMS and NPAC user complaints
- List of cleared trouble reports

12.20 Facilities Requirements

The NPAC must provide an actual or virtual point of presence in the Chicago LATA 358 in Illinois by which service providers can connect to the NPAC SMS. Service providers will be able to connect to the NPAC SMS by connecting to either the NPAC SMS facility location or to the Chicago LATA point of presence

The physical location of the NPAC facility is at the discretion of the NPAC contractor. The only limitation is that the facility must be within the continental United States. Identification of the proposed NPAC location must be included as part of the bidder's response.

The facility may be a separate building or be part of a larger facility owned or leased by the NPAC contractor. If the NPAC is located within a larger facility, space allocated to the NPAC must have the following characteristics:

- Be dedicated entirely for NPAC use
- Be a distinguishable area, separate from other parts of the facility by use of secure access points
- Be contiguous space so that all NPAC staff members are physically located within the same secure area

- Serve as the primary (and, if applicable, secondary) work areas for all NPAC functions to be performed
- Have sufficient and suitable telecommunications links available with diverse routing disaster protection
- Provide sufficient backup power to maintain operation through electrical outages of at least eight hours

The amount of space allocated by the NPAC contractor must be specified in proposals. The specification must include square footage and work space layouts for each of the NPAC staff members. It is recommended that each functional area specified have its own distinct work area. Any equipment required by the different groups should be located within the individual functional group work area, except for equipment deemed to be common to multiple NPAC groups (e.g., high-speed printers, data communication controllers) which may be located in a common area.

12.21 Telecommunications Requirements

Key Requirements

- Individual phone lines for staff members
- hour hotline
- Voice messaging system
- Data communication facilities
- FAX Machine
- Each NPAC staff member must have an individual phone line to their desk. All phone lines must provide the capability of transferring a call to any other phone line within the NPAC.
- The NPAC must have a primary phone number (hotline) with direct inward dialing functionality. Staff members must be able to answer the hotline directly from their desks. This number will be the primary means of contact for the NPAC SMS users who have questions.
- The phone system must provide the capability to allow a caller to leave a message easily. This can be accomplished by an electronic messaging system that allows the caller to leave a message for the person called. In any case, a visual indication that a message has been left is required. The caller must be able to reach a "live" NPAC staff member at all times.
- The NPAC must provide a 24-hour hodine that will give the NPAC SMS user:
- Guaranteed Access to an Actual NPAC Staff Member 24 Hours a Day
- The latest NPAC SMS status available at times when the system may be unavailable during scheduled or unscheduled downtime.
- The choice of voice communication architecture, vendors, equipment, and services is totally at the discretion of the NPAC contractor. The goal of these choices should be to best meet the functionality and service requirements described above. The NPAC contractor will be responsible for the cost and services management of its voice communication facilities. The NPAC contractor will also be responsible for meeting or exceeding the required qualitative and quantitative performance levels that will be part

of the regular service monitoring audits. Bidder response to this RFP must include a description of the proposed NPAC voice communication facilities to be implemented.

- Procurement and management of the data communication facilities required between the NPAC contractor, the data center, and the system vendor are the responsibility of the NPAC contractor. The contractor must provide redundant data communication facilities to provide for disaster recovery due to facility outages. It will be the responsibility of NPAC contractor to meet the data communication specifications of the NPACSMS system vendor. Data Communication must also include the ability to input into the appropriate trouble reporting systems.

12.22 Staffing

Key Requirements

- Please provide proposed staffing profiles and staffing levels. This must be part of the bidder's initial response.
- Please indicate whether you are using part and full-time employees and also the screening process for determining employment.

12.23 Service Objectives

NPAC Availability

NPAC hours of operation will be 24 hours a day, seven days a week. Staffing at the facility will be at appropriate levels to ensure quick response to user needs at any time of the day or week.

Quality of Service

The goal of the NPAC is to provide high quality NPACSMS support and user support. NPAC will play a key role in the achievement of error free, ubiquitous ported local number service provisioning on the part of service providers. In this role, the NPAC contractor must, at all times, be mindful of the revenue and time sensitive nature of the support services provided to users.

Performance Standards

The NPAC contractor performance will be monitored in accordance with the standards proposed as part of the bidder's response and then negotiated following the contractor selection. These NPAC service standards must tie together the following three quality--of-service components: Performance standards for NPAC procedural tasks (illustrative task standards available upon request) Bidder's quality assurance and control guidelines upon which NPAC staff members base their individual performance objectives NPACcontractor defined performance evaluation process that, through self-monitoring, provides ongoing measurements of how well NPAC service objectives are being met.

The bidder's response must address standards addressing each of the following criteria:

- Service consistency
- Service reliability
- Service response time

The NPAC contractor's performance will be evaluated by the Contracting Party. The process will consist of both quantitative and qualitative assessments.

Requirements Checklist

This section provides a summary checklist of the requirements and responsibilities of NPAC. Respondents are required to review the applicable information in each of the references cited and are required to provide an RFP response affirming compliance (or non-compliance) with the specification. Affirmative statements will require compliance in generally available production system(s) to meet the 4Q96 in-service date. If not able to state compliance with all of a reference's requirements to meet such date, the responding vendor shall provide the earliest date that a compliant product can be delivered.

- Does (will) the product comply?

Product compliant delivery date

References

	Product compliant delivery date	**Does (will) the product comply?**
12.2 Logon Administration		
Assist with new logon requests		Yes___ No___
Verify logon signature approval		Yes___ No___
Initialize logon ID, password and security level		Yes___ No___
Update database and add new users		Yes___ No___
Notify user of logon activation		Yes___ No___
Resolve problems with existing logon IDs or passwords		Yes___ No___
12.3 Customer Record Security		
Establish user boundaries through user access permission classes		Yes___ No___
Assign new users to the correct security permission class		Yes___ No___
Exercise absolute control of access to customer records		Yes___ No___
Monitor and report unauthorized system access attempts		Yes___ No___
12.4 Scheduled System Unavailability Notification		
Notify users in advance of planned or known system unavailability		Yes___ No___

Does (will) the product complv? Yes___ No___

_____

12.5 Software Release Acceptance Testing

Update software test plans Yes___ No___ _____

Allocate staff for performing tests Yes___ No___ _____

Execute test plans Yes___ No___ _____

Generate and resolve testing trouble reports Yes___ No___ _____

Document test results Yes___ No___ _____

Certify NPAC SMS software and release for operation Yes___ No___ _____

12.6 Administration of Global Tables

Create and maintain NPAC SMS data tables Yes___ No___ _____

Map table information to appropriate codes Yes___ No___ _____

(i.e., NPA, NXX, LRN)

Create and maintain descriptive data table labels Yes___ No___ _____

12.7 NPA Split/Mass Changes Administration

Maintain a close working relationship with organizations Yes___ No___ _____

responsible for NPA split/mass changes scheduling Yes___ No___ _____

Analyze split impact on NPAC SMS administrative tables Yes___ No___ _____

Analyze split impact on NPAC SMS customa records Yes___ No___ _____

Notify pending split to appropriate service provider service Yes___ No___ _____

administration centers

Coordinate with data center vendor to execute Yes___ No___ _____

NPAC SMS programs required to perform table and Yes___ No___ _____

record modifications

12.8 User Problem Resolution

Resolve customer record access problems Yes___ No___ _____

Clarify feature capabilities for users Yes___ No___ _____

Resolve customer record input and modification problems Yes___ No___ _____

Perform acceptance testing for new software releases Yes___
No___ _____

12.9 Software Release Acceptance Testing

Update software test plans Yes___
No___ _____

Allocate staff for performing tests Yes___
No___ _____

Execute test plans Yes___
No___ _____

Generate and resolve testing trouble reports Yes___
No___ _____

Document test results Yes___
No___ _____

Certify NPAC SMS software and release for operation Yes___
No___ _____

12.10 Software Update Notification

Notify users of upcoming NPAC SMS software releases Yes___ No___ _____

12.11 Training Administration

Serve as primary contact for course schedules/registration information Yes___ No___ _____

Ensure availability of all NPAC SMS training Yes___ No___ _____

12.12 Document Order Administration

Process documentation requests Yes___ No___ _____

Provide billing documentation Yes___ No___ _____

Initiate documentation update distribution Yes___ No___ _____

Provide documentation description, ordering information and price list literature Yes___ No___ _____

12.13 Training and Documentation User Feedback

Getting appropriate user recommendations reflected in NPAC SMS system documentation and training material Yes___ No___ _____

12.14 SCP Download Problem Resolution

Analyze and resolve exception report issues resulting from unsuccessful SCP updates Yes___ No___ _____

12.15 Report Administration

Generate and distribute NPAC SMS reports to all requesting users who are entitled to receive reports Yes___ No___ _____

Validate the accuracy of report contents Yes___ No___ _____

Generate and distribute reports to NPAC SMS users who are entitled to receive reports and do not have local print facilities Yes___ No___ Yes___ No___ _____

Resolve report interpretation problems

12.16 Failure Recovery Administration and User Notification

Notify all NPAC SMS user groups of an unscheduled system Yes___ No___ _____

shutdown or failure

12.17 Interface Monitoring

Assist in the resolution of data communication problems Yes___ No___ _____

with other NPAC SMS service systems (SPs, Operator Service Systems, RAOs, etc.)

Provide technical assistance to NPAC SMS users Yes___ No_____

experiencing problems accessing the system

Generate automatic audit reports

12.18 Software Release Acceptance Testing

Update software test plans Yes___ No___ _____

Allocate staff for performing tests Yes___ No___ _____

Execute test plans Yes___ No_____

Generate and resolve testing trouble reports Yes___ No___ _____

Document test results Yes___ No_____

Certify NPAC SMS software and release for operation Yes___ No___ _____

12.19 Administration

Plan NPAC staff for software acceptance testing, ensure problem report acceptance results, and resolution of discrepancies Yes___ No___ _____

Schedule staff training for new software features and updates Yes___ No___ _____

Analyze documentation and training impact Yes___ No___ _____

Coordinate testing and cutover with NPAC SMS data center operations Yes___ No___ _____

Coordinate critical software release cutover Yes___ No___ _____

Provide monthly billing for service provider and SCP owner/operator NPAC usage Yes___ No___ _____

Manage NPAC accounts receivable collection Yes___ No___ _____

Manage NPAC accounts payable responsibilities Yes___
No___ _____
Resolve any NPAC billing disputes Yes___
No___ _____
Process bills to NPAC from data center operations and Yes___
No___ _____
system vendor for support services
Adjust staffing level based on forecast system usage Yes___
No___ _____
demands
Plan capital equipment based on required staffing levels and Yes___
No___ _____
NPAC performance standards
Manage NPAC facilities Yes___
No_____
Monthly status reports on total billing, summary of
customer service activities, transactions, and trouble reports,
summary of administrative
and other support activities

List of trouble reports, with a breakdown between NPAC SMS Yes___ No___

_____

and NPAC user complaints

List of cleared trouble reports Yes___ No___

_____

12.20 Facilities Requirements

Be dedicated entirely for NPAC use Yes___ No___

_____

Be a distinguishable area, separate from other parts of the facility by use of secure access points Yes___ No___

_____

Be contiguous space so that all NPAC staff members are

physically located within the same secure area Yes___ No___

_____

Serve as the primary (and, if applicable, secondary) work areas for all NPAC functions to be performed Yes___ No___

_____

Have sufficient and suitable telecommunications links available with diverse routing disaster protection Yes___ No___

_____

Provide sufficient backup power to maintain operation through electrical outages of at least tight hours

12.21 Telecommunications Requirements

Individual phone lines for staff members Yes___ No___

_____

24 hour hotine Yes___ No___

_____

Voice Messaging System Yes___ No___

_____

Data communication facilities Yes___ No___

_____

12.22 Staffing

Permanent, full time employees Yes___ No___

_____

Responsibilities dedicated to the NPAC Yes___ No___

_____

Background check Yes___ No___

_____

12.23 Service Objectives

NPAC availability 24 hours a day, seven days a week Yes___ No___ _____

Service consistency Yes___ No___ _____

Service reliability Yes___ No___ _____

Service response time Yes___ No___ _____

SECTION 13: FUTURE CONSIDERATION

The future of number portability, such as the number of service providers and possible expansion to geographic and service portability, and number administration are not known at this time. The SMS platform should not preclude future expansion to adapt to additional needs as they arise. Specific impacts that may occur are as follows:

1. Expansion to allow additional service providers. This will increase the number of ports needed for the links and the number of service providers sending updates and receiving broadcasts.
2. Expansion to other states: This will require an increase in the size of the database, and an increase in both the number of updates and the number of broadcasts. The number of service providers using the SMS may also increase.
3. Geographic number portability: This will require an increase in the size of the database, and an increase in both the number of updates and the number of broadcasts. There may also be interfaces between regional SMSs. Geographic portability may be done in stages, such as initially being geographic portability beyond current rate centers but within a specific region.
4. Pooled NXXs: This will require an increase in the size of the database due to all numbers within a shared No being in the database, and an increase in both the number of updates and the number of broadcasts. This may also require some number administration in the SMS.
5. Overlays of NPA-NXXs: The NPAC SMS will be required to adapt to changes, if any, resulting from overlays.
6. Expansion for use by wireless service providers: This may require new data fields and an increase in the number of service providers using the SMS.
7. Expansion to include data related to resellers. This may require data indicating the reseller, if any for telephone numbers and will increase the size of the database. Resellers may also need to access the database.

The above are not intended as requirements on the SMS, but only as information on possible future needs. Vendors are requested to describe how the NPAC and SMS can be adapted to accommodate the above situations. This information does not imply future obligation on the group to contract with the selected vendor for any future needs.